



19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

12 Offenlegungsschrift
10 DE 101 41 438 A 1

51 Int. Cl.⁷:
G 06 F 12/14
// H04M 1/66, H04Q
7/32

21 Aktenzeichen: 101 41 438.2
22 Anmeldetag: 23. 8. 2001
43 Offenlegungstag: 28. 3. 2002

DE 101 41 438 A 1

30 Unionspriorität:
00-262445 31. 08. 2000 JP
71 Anmelder:
Mitsubishi Denki K.K., Tokio/Tokyo, JP
74 Vertreter:
Prüfer und Kollegen, 81545 München

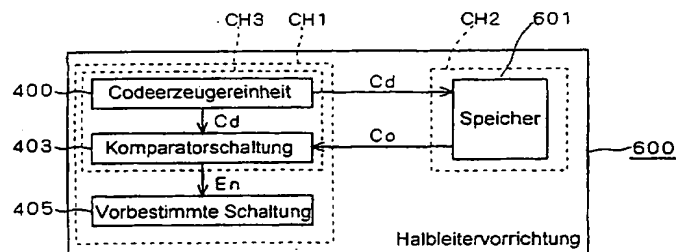
72 Erfinder:
Maeda, Shigenobu, Tokio/Tokyo, JP

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

54 Halbleitervorrichtung und Anschlußeinrichtung

57 Eine Codeerzeugereinheit (400) erzeugt einen Identifikationscode (Cd), der einem Halbleitersubstrat (CH1 und CH3) inhärent ist. Ein in einem anderen Halbleitersubstrat (CH2) gebildeter Speicher speichert den Identifikationscode (Cd) als einen Speichercode (Co). Der Identifikationscode wird von der Codeerzeugereinheit (400) in den Speicher (601) vor dem Versenden einer Halbleitervorrichtung (600) als ein Produkt geschrieben. Eine Komparatorschaltung (403) vergleicht den Identifikationscode (Cd) mit dem Speichercode (Co) und stoppt einige Tätigkeiten einer vorbestimmten Schaltung (405), wenn die zwei Codes nicht miteinander übereinstimmen. Mit diesem Aufbau ist eine höhere technische Barriere (Sicherheit) gegen betrügerische Benutzung eines Gerätes und der Halbleitervorrichtung durch Ersetzen des Halbleitersubstrates erzielbar.



DE 101 41 438 A 1

[0001] Die vorliegende Erfindung bezieht sich auf eine Halbleitervorrichtung und eine Anschlußeinrichtung, die die Halbleitervorrichtung verwendet.

[0002] Es wird gesagt, daß eine betrügerische Benutzung einer Anschlußeinrichtung wie ein Mobiltelefon (Handy), d. h. eine ungesetzliche Tätigkeit des Vermeidens der Pflicht des Zahlens unter dem Vorwand, daß die Anschlußeinrichtung des Benutzers die Anschlußeinrichtung eines anderen ist, kürzlich zugenommen hat. Obwohl natürlich die betrügerische Benutzung durch Sozialmaßnahmen gesteuert werden soll, indem eine gesetzliche Strafe auferlegt wird, ist anerkannt, daß zur gleichen Zeit eine technische Schwierigkeit der betrügerischen Benutzung, mit andern Worten eine höhere technische Hürde (Sicherheit) gegen die betrügerische Benutzung eine besonders wichtige Gegenmaßnahme zum Verhindern des Verbrechens ist.

[0003] Fig. 64 ist eine Darstellung, die aus einem Artikel aus "Nikkei Electronic" am 08. Februar 1999 (Nr. 736), S. 155-162 (Druckschrift 1) genommen ist, die ein Beispiel von gegenwärtigen Gegenmaßnahmen zur Betrugsverhinderung bei Mobiltelefonen zeigt. Wie in der Druckschrift 1 beschrieben ist, ist das Verfahren von Fig. 64 eines mit dem höchsten Sicherheitsstandard unter den gegenwärtigen Gegenmaßnahmen zur Betrugsverhinderung, indem ein Verfahren der "Echtheitsbestätigung" benutzt wird.

[0004] Bei diesem Verfahren werden eine elektronische Seriennummer (ESN) eines Mobiltelefones, geteilte Sicherheitsdaten (SSD), die von dem Mobiltelefon und einem Bestätigungszentrum eines gemeinsamen Kommunikationsträgers geteilt werden, und eine Mobilidentifikationsnummer (MIN) jedem Mobiltelefon zugeordnet. Diese Identifikationsnummern werden in Chiffre, die als AUTHREQ bezeichnet wird, auf der Grundlage des CAVE-(Mobilbestätigung und Stimmenverschlüsselung)Algorithmus codiert. Bei der Verschlüsselung wird eine Zufallszahl, die als RAND bezeichnet wird, die von einem Mobilvermittlungszentrum des gemeinsamen Kommunikationsträgers ausgegeben wird, benutzt.

[0005] Der gemeinsame Kommunikationsträger decodiert die Chiffre AUTHREQ, die von dem Mobiltelefon übertragen wird, auf der Grundlage des CAVE-Algorithmus. Die durch die Decodierung erzielte Identifikationsnummer wird mit einer Identifikationsnummer verglichen, die in den gemeinsamen Geheimdaten (SSD) enthalten ist, die nur von dem Bestätigungszentrum gekannt wird, und es wird eine Beurteilung durchgeführt, ob die Kommunikation erlaubt werden soll oder nicht in Abhängigkeit des Vergleichsergebnisses. Somit wird eine Überprüfung, ob der Benutzer des Mobiltelefones autorisiert ist oder nicht, durchgeführt, d. h. es wird eine Bestätigung auf der Grundlage der gemeinsamen Geheimdaten (SSD) durchgeführt, die nur von dem Mobiltelefon und dem gemeinsamen Kommunikationsträger geteilt wird.

[0006] Es wird jedoch gesagt, daß die illegale Tätigkeit durch die betrügerische Benutzung, die dem Bestätigungssystem von Fig. 64 ausweicht, das als gegenwärtige Gegenmaßnahme zur Betrugsverhinderung mit dem höchsten Sicherheitsgrad angesehen wird, vorherrscht. Weiter wird gesagt, daß einer der technischen Ursachen die ist, daß die dem Mobiltelefon gegebene Identifikationsnummer in einen Flash-Speicher (Flash-ROM) geschrieben ist, der wiederbeschreibbar ist, wie in der Druckschrift 1 beschrieben ist.

[0007] Fig. 65 ist ein Blockschaltbild, das kurz den inneren Aufbau eines Mobiltelefones zeigt. Ein Mobiltelefon 903 weist einen Flash-Speicher 908 als auch eine Kommunikationsschaltung 907 auf. Die Kommunikationsschaltung

907 wird gemäß einem in den Flash-Speicher 908 geschriebenen Programm tätig. Die Identifikationsnummer ID ist ebenfalls in dem Flash-Speicher 908 gespeichert, und die Kommunikationsschaltung 907 führt das Codieren der aus dem Flash-Speicher 908 gelesenen Identifikationsnummer ID durch und überträgt eine Chiffre AUTHREQ, die durch Codieren erzielt wird, zu dem gemeinsamen Kommunikationsträger.

[0008] Der Grund, aus dem der wiederbeschreibbare Flash-Speicher 908 als ein Speichermedium benutzt wird, ist der, daß es notwendig ist, auf eine Programmänderung zu reagieren, die durch den gemeinsamen Kommunikationsträger durchgeführt wird, z. B. eine Änderung in ein Programm für ein neues Kommunikationssystem. Weiter verhindert die Benutzung eines nicht wiederbeschreibbaren Masken-ROM nicht nur die Programmänderung, sondern sie benötigt die Benutzung verschiedener Maskenmuster entsprechend der Identifikationsnummern, die sich von einer Einrichtung zu der anderen bei dem Herstellungsvorgang des Masken-ROM zum Aufzeichnen der Identifikationsnummern unterscheiden, wodurch die Herstellungseffektivität verschlechtert wird und die Herstellungskosten vergrößert werden.

[0009] Die Anmeldung (JP 11-178173 A: Druckschrift 2) der gegenwärtigen Anmelderin offenbart eine Technik zum Lösen der obigen Ursache, bei der ein Halbleiterelement mit einer polykristallinen Substanz in einem Halbleitersubstrat gebildet wird und eine Variation der elektrischen Eigenschaften, die durch eine Variation der Kristallstrukturen der polykristallinen Substanz verursacht wird, zum Erzeugen einer Identifikationsnummer benutzt wird.

[0010] Andererseits ist zusätzlich zu der oben beschriebenen betrügerischen Benutzung durch Neuschreiben einer Identifikationsnummer eine andere Art von betrügerischer Benutzung einer Anschlußeinrichtung bekannt durch Ersetzen eines Halbleitersubstrates (Halbleiterchip), der in einer Anschlußeinrichtung eingebaut ist. Genauer, die betrügerische Benutzung durch Ersetzen eines Halbleitersubstrates, in dem eine Identifikationsnummer aufgezeichnet ist, durch ein Halbleitersubstrat, in dem eine andere Identifikationsnummer aufgezeichnet ist, so daß vorgegeben wird, daß die eigene Anschlußeinrichtung des Benutzers die eines anderen ist, ist aufgetaucht. Weiter ist ein Verbrechen bekannt, einen illegalen Gewinn durch die betrügerische Benutzung zu erzielen durch Ersetzen des Halbleitersubstrates in einem allgemeinen Gerät einer Halbleitervorrichtung, die in einer Spielmaschine zum Glücksspielen ("PACHINKO Maschine" in Japan als gutes Beispiel) und ähnlichem enthalten ist.

[0011] Weiterhin ist eine noch andere Art der betrügerischen Benutzung einer Anschlußeinrichtung bekannt, die eine Funkkommunikation durch einen gemeinsamen Kommunikationsträger (z. B. ein Mobiltelefon) durchführt zum Vermeiden der Pflicht des Bezahlens unter dem Vorwand, daß die Anschlußeinrichtung verlorengegangen ist, während sie benutzt wurde.

[0012] Es ist eine Aufgabe der vorliegenden Erfindung, eine Halbleitervorrichtung und eine Anschlußeinrichtung vorzusehen zum Vergrößern der technischen Barriere (Sicherheit) gegen verschiedene Arten betrügerischer Benutzung. Dabei soll eine höhere Bequemlichkeit bei der Funkkommunikation unter Verwendung dieser Technik erzielt werden.

[0013] Diese Aufgabe wird gelöst durch eine Halbleitervorrichtung mit den Merkmalen des Anspruches 1.

[0014] Die vorliegende Erfindung ist insbesondere auf eine Halbleitervorrichtung gerichtet. Gemäß einem ersten Aspekt der vorliegenden Erfindung weist die Halbleitervorrichtung auf:

$N(1 \leq N)$ Codiererzeugereinheit, die in N Halbleitersubstrat in einer Eins-zu-Eins-Beziehung gebildet ist, wobei jede der N Codeerzeugereinheit aufgebaut ist zum Erzeugen eines Identifikationscodes, der einem entsprechenden Halbleitersubstrat innewohnt; und N Speicher, der in einer Eins-zu-Eins-Beziehung zu dem N Identifikationscode gebildet ist, wobei jeder der N Speicher einen Code speichert, der mit einem entsprechenden Identifikationscode übereinstimmt, als Speichercode, und jeder der N Speicher in einem anderen Halbleitersubstrat als ein entsprechendes Halbleitersubstrat gebildet ist.

[0015] Gemäß einem zweiten Aspekt der vorliegenden Erfindung weist in der Halbleitervorrichtung nach dem ersten Aspekt jeder der N Speicher einen OTPROM auf, der den Speichercode speichert.

[0016] Gemäß einem dritten Aspekt der vorliegenden Erfindung weist bei der Halbleitervorrichtung nach dem ersten oder zweiten Aspekt jede der N Codeerzeugereinheit ein Halbleiterelement und eine Codeschaltung, die zum Umwandeln einer elektrischen Eigenschaft des Halbleiterelementes in ein digitales Signal aufgebaut ist, so daß der Wert des digitalen Signales mit der Variation der elektrischen Eigenschaft des Halbleiterelementes variiert, zum Erzeugen des Identifikationscodes und Ausgeben des Identifikationscodes, auf.

[0017] Gemäß einem vierten Aspekt der vorliegenden Erfindung weist in der Halbleitervorrichtung des dritten Aspektes das Halbleiterelement eine polykristalline Substanz auf, und die Variation der elektrischen Eigenschaft des Halbleiterelementes wird durch Variation der Kristallstruktur der polykristallinen Substanz verursacht.

[0018] Gemäß einem fünften Aspekt der vorliegenden Erfindung weist bei der Halbleitervorrichtung des ersten oder zweiten Aspektes jede der N Codeerzeugereinheit einen OTPROM auf, der den Identifikationscode speichert.

[0019] Gemäß einem sechsten Aspekt der vorliegenden Erfindung weist die Halbleitervorrichtung nach einem des ersten bis fünften Aspektes weiter auf: N Komperatorschaltung, die in Eins-zu-Eins-Beziehung zu dem N Identifikationscode gebildet ist, wobei jede der N Komperatorschaltung aufgebaut ist zum Vergleichen eines entsprechenden Identifikationscodes und eines entsprechenden Speichercode zum Beurteilen dadurch, ob diese Codes miteinander übereinstimmen oder nicht, und zum Ausgeben eines Freigabesignales, das das Beurteilungsergebnis darstellt.

[0020] Gemäß einem siebten Aspekt der vorliegenden Erfindung ist bei der Halbleitervorrichtung des sechsten Aspektes jede der N Komperatorschaltung in dem Halbleitersubstrat entsprechend einem entsprechenden Identifikationscode gebildet, der zu vergleichen ist.

[0021] Gemäß einem achten Aspekt der Erfindung weist die Halbleitervorrichtung des siebten Aspektes weiter auf: N Schlüsselerzeugereinheit, N Verschlüsselungsschaltung und N Decodierschaltung, die in einer Eins-zu-Eins-Entsprechung zu dem N Identifikationscode gebildet sind, wobei jede der N Schlüsselerzeugereinheit, jede der N Verschlüsselungsschaltung und jede der N Decodierschaltung in dem Halbleitersubstrat entsprechend eines entsprechenden Identifikationscodes gebildet sind, und bei der Halbleitervorrichtung nach dem achten Aspekt erzeugt jede der N Schlüsselerzeugereinheit einen Schlüssel zum Verschlüsseln innewohnend in einem entsprechenden Halbleitersubstrat, jede der N Verschlüsselungsschaltung verschlüsselt den Identifikationscode, der von der Codeerzeugereinheit erzeugt ist, die in dem entsprechenden Halbleitersubstrat gebildet ist, auf der Grundlage eines entsprechenden Schlüssels und überträgt den Identifikationscode der verschlüsselten Form zu dem entsprechenden Speicher, jeder der N Speicher spei-

chert den Identifikationscode der verschlüsselten Form, der von der entsprechenden Verschlüsselungsschaltung ausgegeben ist, als den Speichercode der verschlüsselten Form, jede der N Decodierschaltung decodiert den Speichercode der verschlüsselten Form, der in einem entsprechenden Speicher gespeichert ist, auf der Grundlage eines entsprechenden Schlüssels, und jede der N Komperatorschaltung vergleicht den Identifikationscode, der von einer entsprechenden Codeerzeugereinheit erzeugt ist, mit dem Speichercode, der durch eine entsprechende Decodierschaltung decodiert ist.

[0022] Gemäß einem neunten Aspekt der vorliegenden Erfindung weist bei der Halbleitervorrichtung des achten Aspektes jede N Schlüsselerzeugereinheit ein anderes Halbleiterelement; eine andere Codierschaltung zum Umwandeln einer elektrischen Eigenschaft des anderen Halbleiterelementes in ein anderes digitales Signal so, daß ein Wert des anderen Digitalsignales mit der Variation der elektrischen Eigenschaft des anderen Halbleiterelementes variiert zum Erzeugen des Schlüssels und Ausgeben des Schlüssels auf.

[0023] Gemäß einem zehnten Aspekt der vorliegenden Erfindung weist bei der Halbleitervorrichtung des neunten Aspektes das andere Halbleiterelement eine andere polykristalline Substanz auf, und die Variation der elektrischen Eigenschaft des anderen Halbleiterelementes wird durch die Variation der Kristallstruktur der anderen polykristallinen Substanz verursacht.

[0024] Gemäß einem elften Aspekt der vorliegenden Erfindung weist bei der Halbleitervorrichtung des achten Aspektes jede der N Schlüsselerzeugereinheit einen OTPROM auf, der den Schlüssel speichert.

[0025] Gemäß einem zwölften Aspekt der vorliegenden Erfindung weist die Halbleitervorrichtung nach einem des siebten bis elften Aspektes weiter auf N Umschalterschaltung, die in einer Eins-zu-Eins-Entsprechung zu den N Identifikationscode gebildet sind, wobei jede der N Umschalterschaltung in dem Halbleitersubstrat in Entsprechung zu einem entsprechenden Identifikationscode gebildet ist, jede der N Umschalterschaltung so aufgebaut ist, daß exklusiv eine Übertragung eines entsprechenden Identifikationscodes, der durch eine entsprechende Codeerzeugereinheit erzeugt ist, zu einem entsprechenden Speicher und eine Eingabe des in dem entsprechenden Speicher gespeicherten Speichercode zu einer entsprechenden Komperatorschaltung durchführt.

[0026] Gemäß einem dreizehnten Aspekt der vorliegenden Erfindung weist die Halbleitervorrichtung nach einem des sechsten bis zwölften Aspektes weiter auf eine vorbestimmte Schaltung mit einem Schaltungsabschnitt, der selektiv in einen aktiven oder einen inaktiven Zustand kommt in Abhängigkeit des N Freigabesignales, das entsprechend den N Identifikationscode entspricht.

[0027] Gemäß einem vierzehnten Aspekt der vorliegenden Erfindung ist bei der Halbleitervorrichtung des dreizehnten Aspektes die vorbestimmte Schaltung in einem der N Halbleitersubstrat zusammen mit der entsprechenden Komperatorschaltung gebildet.

[0028] Gemäß einem fünfzehnten Aspekt der vorliegenden Erfindung ist bei der Halbleitervorrichtung nach einem des ersten bis vierzehnten Aspektes die Zeit $N = 1$.

[0029] Gemäß einem sechzehnten Aspekt der vorliegenden Erfindung ist bei der Halbleitervorrichtung nach einem des ersten bis vierzehnten Aspektes die Zahl $N = 2$, und jede der N Codeerzeugereinheit und des entsprechenden Speichers sind entsprechend in einem und dem anderen der N Halbleitersubstrate gebildet.

[0030] Die vorliegende Erfindung ist auch auf eine Anschlußeinrichtung gerichtet. Gemäß einem siebzehnten

Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung auf: eine Schlüsselerzeugereinheit mit einem Halbleiterelement und einer Codierschaltung, die aufgebaut ist zum Umwandeln einer elektrischen Eigenschaft des Halbleiterelementes in ein digitales Signal so, daß ein Wert des digitalen Signales mit der Variation der elektrischen Eigenschaft des Halbleiterelementes variiert zum Erzeugen eines Schlüssels zum Verschlüsseln und Ausgeben des Schlüssels; eine Verschlüsselungsschaltung, die aufgebaut ist zum Verschlüsseln von Übertragungsdaten auf der Grundlage des Schlüssels; und eine Decodierschaltung zum Decodieren empfangener Daten auf der Grundlage des Schlüssels.

[0031] Gemäß einem achtzehnten Aspekt der vorliegenden Erfindung sind bei der Halbleitervorrichtung des siebzehnten Aspektes die Verschlüsselungsschaltung und die Decodierschaltung in einem Hauptkörperabschnitt eingebaut, und die Schlüsselerzeugereinheit ist in einen Hilfsabschnitt eingebaut, der von dem Hauptkörperabschnitt lösbar ist.

[0032] Gemäß einem neunzehnten Aspekt der vorliegenden Erfindung ist bei der Halbleitervorrichtung des achtzehnten Aspektes der Hilfsabschnitt eines IC-Karte.

[0033] Gemäß einem zwanzigsten Aspekt der vorliegenden Erfindung weist bei der Halbleitervorrichtung nach einem des siebzehnten bis neunzehnten Aspektes das Halbleiterelement eine polykristalline Substanz auf, und die Variation der elektrischen Eigenschaft des Halbleiterelementes wird durch eine Variation in der Kristallstruktur der polykristallinen Substanz verursacht.

[0034] Gemäß einem einundzwanzigsten Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung auf: die Halbleitervorrichtung, wie sie in den dreizehnten oder vierzehnten Aspekt definiert ist, und bei der Anschlußeinrichtung des einundzwanzigsten Aspektes ist die vorbestimmte Schaltung eine Kommunikationsschaltung zum Übertragen und Empfangen eines Signales nach außen und von außen, und mindestens eine der Übertragung und des Empfangens wird gestoppt, wenn das N Freigabesignal eine Nichtübereinstimmung zwischen mindestens einem der N Identifikationscodes und eines entsprechenden Speichercode anzeigt.

[0035] Gemäß einem zweiundzwanzigsten Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung auf: die Halbleitervorrichtung, wie sie in einem des sechsten bis zwölften Aspekt definiert ist; und eine Kommunikationsschaltung, die zum Übertragen und Empfangen eines Signales nach außen und von außen, und bei der Anschlußeinrichtung des zweiundzwanzigsten Aspektes überträgt die Kommunikationsschaltung das N Freigabesignal als Teil des Signales nach außen.

[0036] Gemäß einem dreiundzwanzigsten Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung auf: die Halbleitervorrichtung, wie sie in einem des ersten bis fünften Aspektes definiert ist; und eine Kommunikationsschaltung, die zum Übertragen und Empfangen eines Signales nach außen und von außen aufgebaut ist, und bei der Anschlußeinrichtung des dreiundzwanzigsten Aspektes überträgt die Kommunikationsschaltung den N Identifikationscode und den N Speichercode als Teil des Signales nach außen.

[0037] Gemäß einem vierundzwanzigsten Aspekt der vorliegenden Erfindung ist bei der Anschlußeinrichtung des dreiundzwanzigsten Aspektes die Zahl N gleich 1, die N Codeerzeugereinheit und die Kommunikationsschaltung sind in einen Hauptkörperbereich eingebaut, und der N Speicher ist in einen Hilfsabschnitt eingebaut, der von dem Hauptkörperabschnitt lösbar ist.

[0038] Gemäß einem fünfundzwanzigsten Aspekt der vorliegenden Erfindung ist bei der Anschlußeinrichtung des

vierundzwanzigsten Aspektes in den Hauptkörperabschnitt weiter eine erste Schlüsselerzeugereinheit, die zum Erzeugen eines ersten Schlüssels zum Verschlüsseln aufgebaut ist; und eine erste Verschlüsselungsschaltung, die zum Verschlüsseln des Identifikationscodes, der von der N Codeerzeugereinheit erzeugt ist, auf der Grundlage des ersten Schlüssels aufgebaut ist, eingebaut, und in den Hilfsabschnitt ist weiter eine zweite Schlüsselerzeugereinheit, die zum Erzeugen eines zweiten Schlüssels zur Verschlüsselung aufgebaut ist, und eine zweite Verschlüsselungsschaltung, die zum Verschlüsseln des Speichercode, der in dem N Speicher gespeichert ist, auf der Grundlage des zweiten Schlüssels aufgebaut ist, eingebaut, wobei die erste Verschlüsselungsschaltung auch den Speichercode verschlüsselt, der von der zweiten Verschlüsselungsschaltung verschlüsselt wird, auf der Grundlage des ersten Schlüssels, und die Kommunikationsschaltung den Identifikationscode und den Speichercode beide in einer durch die erste Verschlüsselungsschaltung verschlüsselten Form zu der Außenseite überträgt.

[0039] Gemäß einem sechsundzwanzigsten Aspekt der vorliegenden Erfindung sind bei der Anschlußeinrichtung des fünfundzwanzigsten Aspektes die erste Schlüsselerzeugereinheit und die erste Verschlüsselungsschaltung in dem N Halbleitersubstrat gebildet, in dem die N Codeerzeugereinheit gebildet ist.

[0040] Gemäß einem siebenundzwanzigsten Aspekt der vorliegenden Erfindung sind bei der Anschlußeinrichtung des fünfundzwanzigsten oder sechsundzwanzigsten Aspektes die zweite Schlüsselerzeugereinheit und die zweite Verschlüsselungsschaltung in dem Halbleitersubstrat gebildet, in dem der N Speicher gebildet ist.

[0041] Gemäß einem achtundzwanzigsten Aspekt der vorliegenden Erfindung ist bei der Anschlußeinrichtung nach einem des vierundzwanzigsten bis siebenundzwanzigsten Aspektes in den Hauptkörperabschnitt weiter eine wiederaufladbare Batterie eingebaut, und der Hilfsabschnitt ist ein Batterieladungsgerät, das die Batterie auflädt, wenn er an dem Hauptkörperabschnitt angebracht ist.

[0042] Gemäß einem neunundzwanzigsten Aspekt der vorliegenden Erfindung ist bei der Anschlußeinrichtung nach einem des vierundzwanzigsten bis siebenundzwanzigsten Aspektes der Hilfsabschnitt eine IC-Karte, und der Hauptkörperabschnitt und der Hilfsabschnitt enthalten weiter eine Kommunikationsschnittstelle, die zum Übertragen eines Codes von dem Hilfsabschnitt zu dem Hauptkörperabschnitt drahtlos benutzt wird.

[0043] Nach einem dreißigsten Aspekt der vorliegenden Erfindung ist bei der Anschlußeinrichtung nach einem des zweiundzwanzigsten bis siebenundzwanzigsten Aspektes die Kommunikationsschaltung in einem des N Halbleitersubstrates zusammen mit einer der N Codeerzeugereinheit gebildet.

[0044] Gemäß einem einunddreißigsten Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung auf: eine Kommunikationsschaltung, die zum Durchführen einer Funkverbindung durch eine gemeinsame Kommunikationsträgerschaltung aufgebaut ist, und eine Funkkommunikationsnetzwerkschaltung, die zum Durchführen einer Funkkommunikation aufgebaut ist durch Bilden eines Funkkommunikationsnetzwerkes und nicht durch die gemeinsame Kommunikationsträgerschaltung.

[0045] Gemäß einem zweiunddreißigsten Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung des einunddreißigsten Aspektes weiter auf: eine Auswahlsschaltung, die zum selektiven Durchführen des Verbindens und Trennens eines Pfades aufgebaut ist, durch den Kommunikationssignale übertragen und empfangen werden zwischen

der Kommunikationsschaltung und der Funkkommunikationsnetzwerkschaltung, zum selektiven Herstellen einer Kommunikation zwischen einem Benutzer der Anschlußeinrichtung und einer anderen Person durch das Funkkommunikationsnetzwerk und ein Relais der Kommunikation zwischen einer Mehrzahl von Personen, die nicht der Benutzer der Anschlußeinrichtung sind, durch das Funkkommunikationsnetzwerk.

[0046] Gemäß einem dreiunddreißigsten Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung des zweiunddreißigsten Aspektes weiter auf: eine Schlüsselerzeugereinheit, die zum Erzeugen eines Schlüssels für Verschlüsselung aufgebaut ist, eine Verschlüsselungsschaltung, die zum Verschlüsseln eines Übertragungssignales aufgebaut ist, das von der Kommunikationsschaltung zu der Funkkommunikationsnetzwerkschaltung zu übertragen ist, unter den Kommunikationssignalen auf der Grundlage des Schlüssels; und eine Decodierschaltung, die zum Decodieren eines Empfangssignales aufgebaut ist, das von der Funkkommunikationsnetzwerkschaltung zu der Kommunikationsschaltung zu übertragen ist, aus den Kommunikationssignalen auf der Grundlage des Schlüssels, und bei der Anschlußeinrichtung des dreiunddreißigsten Aspektes weist die Schlüsselerzeugereinheit eine Codeerzeugereinheit, die zum Erzeugen eines Codes zum Identifizieren der Anschlußeinrichtung aufgebaut ist, und eine Schlüsselberechnungseinheit, die zum Berechnen eines gemeinsamen Schlüssels aufgebaut ist, der zwischen dem Benutzer und seinem Kommunikationspartner geteilt werden kann, auf der Grundlage des Codes, der von der Codeerzeugereinheit erzeugt ist, und eines anderen Codes, der von dem Kommunikationspartner durch die Funkkommunikationsnetzwerkschaltung übertragen ist, auf.

[0047] Gemäß einem vierunddreißigsten Aspekt der vorliegenden Erfindung weist bei der Anschlußeinrichtung des dreiunddreißigsten Aspektes die Codeerzeugereinheit ein Halbleiterelement und eine Codierschaltung zum Umwandeln einer elektrischen Eigenschaft des Halbleiterelementes in ein digitales Signal so auf, daß ein Wert des digitalen Signales mit Variation der elektrischen Eigenschaft des Halbleiterelementes variiert zum Erzeugen des Codes und Ausgeben des Codes.

[0048] Gemäß einem fünfunddreißigsten Aspekt der vorliegenden Erfindung weist bei der Anschlußeinrichtung des vierunddreißigsten Aspektes das Halbleiterelement eine polykristalline Substanz auf, und die Variation der elektrischen Eigenschaft des Halbleiterelementes wird durch Variation der Kristallstruktur der polykristallinen Substanz verursacht.

[0049] Gemäß einem sechsunddreißigsten Aspekt der vorliegenden Erfindung weist bei der Anschlußeinrichtung des dreiunddreißigsten Aspektes die Codeerzeugereinheit einen OTPROM auf, der den Code speichert.

[0050] Gemäß einem siebenunddreißigsten Aspekt der vorliegenden Erfindung weist die Anschlußeinrichtung nach einem des zweiunddreißigsten bis sechsunddreißigsten Aspektes weiter auf: einen ersten Mischer und einen zweiten Mischer, die in einen Pfad eingesetzt sind, zum Empfangen des von der Funkkommunikationsnetzwerkschaltung zu der Kommunikationsschaltung zu übertragenen Signales unter den Kommunikationssignalen, und bei der Anschlußeinrichtung des siebenunddreißigsten Aspektes demoduliert der erste Mischer das Empfangssignal, das von der Kommunikationsschaltung empfangen wird, und der zweite Mischer moduliert das demodulierte Empfangssignal mit einer Trägerwelle mit einer Frequenz innerhalb eines Frequenzbandes der Kommunikationsschaltung.

[0051] Die vorliegende Erfindung ist weiter auf ein Kom-

munikationsverfahren gerichtet. Gemäß einem achtunddreißigsten Aspekt der vorliegenden Erfindung weist das Kommunikationsverfahren, das eine gemeinsame Kommunikationsträgerschaltung und die Anschlußeinrichtung ermöglicht, wie sie in dem zweiundzwanzigsten Aspekt definiert ist, zum Durchführen der gegenseitigen Kommunikation die Schritte auf: (a) Übertragen des N Freigabesignales von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgerschaltung und (b) als einen Authentifizierungsschritt das Durchführen einer Authentifizierung, daß ein Benutzer der Anschlußeinrichtung ein autorisierter Benutzer ist, durch die gemeinsame Kommunikationsträgerschaltung, wenn eine Bedingung, daß jedes des N Freigabesignales, das von der gemeinsamen Kommunikationsträgerschaltung empfangen wird, Übereinstimmung zwischen einem entsprechenden Identifikationscode und einem entsprechenden Speichercode bezeichnet, erfüllt ist, und die Authentifizierung nicht durch die gemeinsame Kommunikationsträgerschaltung durchführt, wenn die Bedingung nicht erfüllt ist.

[0052] Gemäß einem neununddreißigsten Aspekt der vorliegenden Erfindung weist das Kommunikationsverfahren, das eine gemeinsame Kommunikationsträgerschaltung und die Anschlußeinrichtung ermöglicht, die in dem dreiundzwanzigsten Aspekt definiert ist, zum Durchführen einer gegenseitigen Kommunikation die Schritte auf: (a) Übertragen des N Identifikationscodes und des N Speichercodes von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgerschaltung; (b) Vergleichen eines jeden des N Identifikationscodes und eines entsprechenden Speichercodes, die empfangen werden, zum Beurteilen, ob jeder der N Identifikationscode und ein entsprechender Speichercode miteinander übereinstimmen oder nicht durch die gemeinsame Kommunikationsträgerschaltung; und (c) als einen Authentifizierungsschritt Durchführen einer Authentifizierung, daß ein Benutzer der Anschlußeinrichtung ein autorisierter Benutzer ist, durch die gemeinsame Kommunikationsträgerschaltung, wenn eine Bedingung, daß ein Beurteilungsergebnis Übereinstimmung zwischen jedem des N Identifikationscodes und einem entsprechenden Speichercode in dem Schritt (b) anzeigt, erfüllt ist, und nicht die Authentifizierung durch die gemeinsame Kommunikationsträgerschaltung ausführt, wenn die Bedingung nicht erfüllt ist.

[0053] Gemäß einem vierzigsten Aspekt der vorliegenden Erfindung weist das Verfahren des neununddreißigsten Aspektes weiter den Schritt auf: (e) Aufzeichnen des N Identifikationscodes und des N Speichercodes, die von der gemeinsamen Kommunikationsträgerschaltung empfangen werden.

[0054] Gemäß einem einundvierzigsten Aspekt der vorliegenden Erfindung zeichnet bei dem Kommunikationsverfahren des neununddreißigsten Aspektes die gemeinsame Kommunikationsträgerschaltung in dem Schritt (c) den N Identifikationscode und den N Speichercode auf, die empfangen werden, wenn die Authentifizierung nicht durchgeführt wird.

[0055] Gemäß einem zweiundvierzigsten Aspekt der vorliegenden Erfindung weist das Kommunikationsverfahren die Schritte auf: (a) Erhalten des N Identifikationscodes der Anschlußeinrichtung, wie sie in dem vierundzwanzigsten Aspekt definiert ist, zum Speichern des N Identifikationscodes als ein zuerst registrierter Code durch die gemeinsame Kommunikationsträgerschaltung; (b) Erhalten des N Speichercodes der Anschlußeinrichtung zum Speichern des N Speichercodes als ein zweiter registrierter Code durch die gemeinsame Kommunikationsträgerschaltung; und (c) als einen Kommunikationsschritt Durchführen der gegenseitigen Kommunikation zwischen der gemeinsamen Kommunikati-

onsträgersausrüstung und der Anschlußeinrichtung nach den Schritten (a) und (b), und in dem Kommunikationsverfahren des zweiundvierzigsten Aspektes weist der Schritt (c) auf (c-1) einen ersten Kommunikationsschritt, der ausgeführt wird, wenn der Hilfsabschnitt nicht an dem Hauptkörperabschnitt angebracht ist, und (c-2) einen zweiten Kommunikationsschritt, der ausgeführt wird, wenn der Hilfsabschnitt an dem Hauptkörperabschnitt angebracht ist, der erste Kommunikationsschritt (c-1) weist die Schritte auf: (c-1-1) Übertragen des N Identifikationscodes von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung; (c-1-2) Vergleichen des N Identifikationscodes, der empfangen wird, mit dem ersten registrierten Code zum Beurteilen, ob der N Identifikationscode und der erste registrierte Code miteinander übereinstimmen oder nicht durch die gemeinsame Kommunikationsträgersausrüstung; und (c-1-3) als ein Authentifizierungsschritt Durchführen einer Authentifizierung, daß ein Benutzer der Anschlußeinrichtung ein autorisierter Benutzer ist, durch die gemeinsame Kommunikationsträgersausrüstung, wenn eine Bedingung, daß das Beurteilungsergebnis Übereinstimmung zwischen dem N Identifizierungscode und dem ersten registrierten Code in dem Schritt (c-1-2) bezeichnet, erfüllt ist, und Nichtausführen der Authentifizierung durch die gemeinsame Kommunikationsträgersausrüstung, wenn die Bedingung nicht erfüllt ist, und der zweite Kommunikationsschritt (c-2) weist die Schritte auf: (c-2-1) Übertragen des N Identifikationscodes und des N Speichercode von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung; (c-2-2) Vergleichen des N Identifikationscode, der empfangen wird, mit dem ersten registrierten Code zum Beurteilen, ob der N Identifikationscode und der erste registrierte Code übereinstimmen oder nicht und Vergleichen des N Speichercode, der empfangen wird, mit dem zweiten registrierten Code, zum Vergleichen, ob der N Speichercode und der zweite registrierte Code miteinander übereinstimmen oder nicht, durch die gemeinsame Kommunikationsträgersausrüstung; und (c-2-3) als ein Hochniveauintifizierungsschritt Durchführen einer Hochniveauintifizierung, daß ein Benutzer der Anschlußeinrichtung ein autorisierter Benutzer ist, durch die gemeinsame Kommunikationsträgersausrüstung, wenn eine Bedingung, daß beide Beurteilungsergebnisse die Übereinstimmungen in dem Schritt (c-2-2) bezeichnen, erfüllt ist, und Nichtdurchführen der Hochniveauintifizierung durch die gemeinsame Kommunikationsträgersausrüstung, wenn die Bedingung nicht erfüllt ist.

[0056] Gemäß einem dreiundvierzigsten Aspekt der vorliegenden Erfindung erhält bei dem Kommunikationsverfahren des zweiundvierzigsten Aspektes die gemeinsame Kommunikationsträgersausrüstung in dem Schritt (b) den N Speichercode der Anschlußeinrichtung durch Ausführen der Kommunikation zwischen der gemeinsamen Kommunikationsträgersausrüstung und der Anschlußeinrichtung, wobei der Hilfsabschnitt an dem Hauptkörperabschnitt angebracht ist.

[0057] Gemäß einem vierundvierzigsten Aspekt der vorliegenden Erfindung weist bei dem Kommunikationsverfahren des zweiundvierzigsten oder dreiundvierzigsten Aspektes der Schritt (c) weiter den Schritt auf: (c3) einen Änderungsschritt des Ändern des zweiten registrierten Codes, wenn der Hilfsabschnitt an dem Hauptkörperabschnitt angebracht ist, der Änderungsschritt (c-3) weist die Schritte auf (c-3-1) Übertragen eines Anforderungssignales, das die Entscheidung der Änderung des zweiten registrierten Codes, des N Identifikationscodes und des N Speichercode darstellt, von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung; (c-3-2) Vergleichen des N Identifikationscode, der empfangen wird, mit dem ersten

registrierten Code, zum Beurteilen, ob der N Identifikationscode und der erste registrierte Code miteinander übereinstimmen oder nicht, und Vergleichen des N Speichercode, der empfangen wird, mit dem zweiten registrierten Code zum Beurteilen, ob der N Speichercode und der zweite registrierte Code miteinander übereinstimmen oder nicht, durch die gemeinsame Kommunikationsträgersausrüstung; (c-3-3) Ermöglichen der Änderung durch die gemeinsame Kommunikationsträgersausrüstung nur, wenn die beiden Beurteilungsergebnisse Übereinstimmung in dem Schritt (c-3-2) bezeichnen; (c-3-4) Ändern des Hilfsabschnittes der Anschlußeinrichtung und Anbringen eines geänderten Hilfsabschnittes an den Hauptkörperabschnitt nach dem Schritt (c-3-3); (c-3-5) Übertragen des N Identifikationscodes und des N Speichercode, die auf der Grundlage des geänderten Hilfsabschnittes geändert sind, von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung nach dem Schritt (c-3-4); und (c-3-6) Aktualisieren des zweiten registrierten Codes durch die gemeinsame Kommunikationsträgersausrüstung mit dem geänderten N Speichercode, der nur empfangen wird, wenn die Änderung in dem Schritt (c-3-3) erlaubt ist.

[0058] Gemäß einem fünfundvierzigsten Aspekt der vorliegenden Erfindung weist das Kommunikationsverfahren die Schritte auf: (a) Erhalten des N Identifikationscodes und des ersten Schlüssels von der Anschlußeinrichtung, wie sie in dem fünfundzwanzigsten Aspekt definiert ist, zum Speichern des N Identifikationscodes und des ersten Schlüssels als einen ersten registrierten Code bzw. registrierten Schlüssel durch die gemeinsame Kommunikationsträgersausrüstung; (b) Erhalten des N Speichercode, der mit dem zweiten Schlüssel der Anschlußeinrichtung verschlüsselt ist, zum Speichern des N Speichercode als ein zweiter registrierter Code durch die gemeinsame Kommunikationsträgersausrüstung; und (c) als ein Kommunikationsschritt Ausführen der gegenseitigen Kommunikation zwischen der gemeinsamen Kommunikationsträgersausrüstung und der Anschlußeinrichtung nach den Schritten (a) und (b), und bei dem Kommunikationsverfahren des fünfundvierzigsten Aspektes weist der Kommunikationsschritt (c) auf (c-1) einen ersten Kommunikationsschritt, der ausgeführt wird, wenn der Hilfsabschnitt nicht an dem Hauptkörperabschnitt angebracht ist, und (c-2) einen zweiten Kommunikationsschritt, der ausgeführt wird, wenn der Hilfsabschnitt an dem Hauptkörperabschnitt angebracht ist, der erste Kommunikationsschritt (c-1) weist die Schritte auf: (c-1-1) Übertragen des N Identifikationscodes in einer durch die erste Verschlüsselungsschaltung verschlüsselten Form von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung; (c-1-2) Decodieren des N Identifikationscodes, der auf der Grundlage des registrierten Schlüssels empfangen wird, und Vergleichen des N Identifizierungscode mit dem ersten registrierten Code zum Beurteilen, ob der N Identifikationscode und der erste registrierte Code miteinander übereinstimmen oder nicht, durch die gemeinsame Kommunikationsträgersausrüstung; und (c-1-3) als ein Authentifizierungsschritt Ausführen einer Authentifizierung, daß ein Benutzer der Anschlußeinrichtung ein autorisierter Benutzer ist, durch die gemeinsame Kommunikationsträgersausrüstung, wenn eine Bedingung, daß das Beurteilungsergebnis die Übereinstimmung zwischen dem N Identifizierungscode und dem ersten registrierten Code in dem Schritt (c-1-2) bezeichnet, erfüllt ist, und Nichtausführen der Authentifizierung durch die gemeinsame Kommunikationsträgersausrüstung, wenn die Bedingung nicht erfüllt ist, und der zweite Kommunikationsschritt (c-2) weist die Schritte auf: (c-2-1) Übertragen des N Identifikationscodes und des N Speichercode beide in einer durch die erste Ver-

schlüsselungsschaltung verschlüsselten Form von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung; (c-2-2) Decodieren des N Identifikationscodes und des N Speicher codes, die empfangen werden, auf der Grundlage des registrierten Schlüssels und Vergleichen des N Identifikationscode mit dem ersten registrierten Code zum Beurteilen, ob der N Identifikationscode und der erste registrierte Code miteinander übereinstimmen oder nicht, und Vergleichen des N Speicher codes mit dem zweiten registrierten Code zum Beurteilen, ob der N Speichercode und der zweite registrierte Code miteinander übereinstimmen oder nicht, durch die gemeinsame Kommunikationsträgersausrüstung; und (c-2-3) als ein Hochniveauintifizierungsschritt Ausführen einer Hochniveauintifizierung, daß ein Benutzer der Anschlußeinrichtung ein autorisierter Benutzer ist, durch die gemeinsame Kommunikationsträgersausrüstung, wenn eine Bedingung, daß beide Beurteilungsergebnisse die Übereinstimmungen in dem Schritt (c-2-2) bezeichnen, erfüllt ist, und Nichtausführen der Hochniveauintifizierung durch die gemeinsame Kommunikationsträgersausrüstung, wenn die Bedingung nicht erfüllt ist.

[0059] Gemäß einem sechsendvierzigsten Aspekt der vorliegenden Erfindung erhält bei dem Kommunikationsverfahren des fünfundvierzigsten Aspektes die gemeinsame Kommunikationsträgersausrüstung in dem Schritt (b) den mit dem zweiten Schlüssel verschlüsselten N Speichercode von der Anschlußeinrichtung durch Durchführen einer Kommunikation zwischen der gemeinsamen Kommunikationsträgersausrüstung und der Anschlußeinrichtung, wobei der Hilfsabschnitt an dem Hauptkörperabschnitt angebracht ist.

[0060] Gemäß einem siebenundvierzigsten Aspekt der vorliegenden Erfindung weist bei dem Kommunikationsverfahren des fünfundvierzigsten oder des sechsendvierzigsten Aspekt der Schritt (c) weiter auf (c-3) einen Änderungsschritt des Änderns des zweiten registrierten Codes, wenn der Hilfsabschnitt an dem Hauptkörperabschnitt angebracht ist, der Änderungsschritt (c-3) weist die Schritte auf: (c-3-1) Übertragen eines Anforderungssignales, daß eine Entscheidung der Änderung des zweiten registrierten Codes darstellt, und des N Identifikationscodes und des N Speicher codes, beide in einer durch die erste Verschlüsselungsschaltung verschlüsselten Form, von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung; (c-3-2) Decodieren des N Identifikationscodes und des N Speicher codes, die empfangen werden auf der Grundlage des registrierten Schlüssels und Vergleichen des N Identifikationscode mit dem ersten registrierten Code zum Beurteilen, ob der N Identifikationscode und der erste registrierte Code miteinander übereinstimmen oder nicht und Vergleichen des N Speicher codes mit dem zweiten registrierten Code zum Beurteilen, ob der N Speichercode und der zweite registrierte Code miteinander übereinstimmen oder nicht, durch die gemeinsame Kommunikationsträgersausrüstung; (c-3-3) Ermöglichen der Änderung durch die gemeinsame Kommunikationsträgersausrüstung nur, wenn eine Bedingung, daß die beiden Beurteilungsergebnisse die Übereinstimmung in dem Schritt (c-3-2) bezeichnen, erfüllt ist; (c-3-4) Ändern des Hilfsabschnittes der Anschlußeinrichtung und Anbringen eines geänderten Hilfsabschnittes an dem Hauptkörperabschnitt nach dem Schritt (c-3-3); (c-3-5) Übertragen des N Identifikationscodes und des N Speicher codes, die auf der Grundlage des geänderten Hilfsabschnittes geändert sind, beide in der durch die erste Verschlüsselungsschaltung verschlüsselten Form von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung nach dem Schritt (c-3-4); und (c-3-6) Aktualisieren des zweiten registrierten Codes durch die gemeinsame Kommunikationsträgersausrüstung mit einem Code, der erhalten wird durch De-

codieren des geänderten N Speicher codes, der empfangen wird, auf der Grundlage des registrierten Schlüssels nur, wenn die Änderung in dem Schritt (c-3-3) erlaubt wird.

[0061] Gemäß einem achtundvierzigsten Aspekt der vorliegenden Erfindung zeichnet bei dem Kommunikationsverfahren nach einem des zweiundvierzigsten bis siebenundvierzigsten Aspektes die gemeinsame Kommunikationsträgersausrüstung in dem Hochniveauintifizierungsschritt jeden Code auf, der mit jedem registrierten Code in dem Schritt (c-2-2) verglichen wird, wenn die Hochniveauintifizierung nicht ausgeführt wird.

[0062] Gemäß einem neunundvierzigsten Aspekt der vorliegenden Erfindung zeichnet bei dem Kommunikationsverfahren nach einem des zweiundvierzigsten bis achtundvierzigsten Aspektes die gemeinsame Kommunikationsträgersausrüstung in dem Hochniveauintifizierungsschritt eine Kommunikationsladung für die Kommunikation davor auf, wie bestätigt, wenn die Hochniveauintifizierung ausgeführt wird.

[0063] Gemäß einem fünfzigsten Aspekt der vorliegenden Erfindung zeichnet bei dem Kommunikationsverfahren nach einem des zweiundvierzigsten bis neunundvierzigsten Aspektes die gemeinsame Kommunikationsträgersausrüstung in dem Hochniveauintifizierungsschritt auf, daß die Hochniveauintifizierung ausgeführt worden ist, wenn die Hochniveauintifizierung durchgeführt wird, und die gemeinsame Kommunikationsträgersausrüstung führt in dem Authentifizierungsschritt die Authentifizierung auf einer weiteren Bedingung aus, daß es aufgezeichnet ist, daß die Hochniveauintifizierung ausgeführt worden ist.

[0064] Gemäß einem einundfünfzigsten Aspekt der vorliegenden Erfindung zeichnet bei dem Kommunikationsverfahren nach einem des zweiundvierzigsten bis fünfzigsten Aspektes die gemeinsame Kommunikationsträgersausrüstung in dem Hochniveauintifizierungsschritt einen Geschäftsvorgang durch die Kommunikation davor auf, wie er abgeschlossen wird, wenn die Hochniveauintifizierung durchgeführt wird, und zeichnet den Geschäftsvorgang durch die Kommunikation davor als nicht geschlossen auf, wenn die Hochniveauintifizierung nicht ausgeführt wird.

[0065] Gemäß einem zweiundfünfzigsten Aspekt der vorliegenden Erfindung fährt bei dem Kommunikationsverfahren nach einem des achtunddreißigsten bis einundfünfzigsten Aspekt die gemeinsame Kommunikationsträgersausrüstung in dem Authentifizierungsschritt die Kommunikation fort, wenn die Authentifizierung durchgeführt wird, und stoppt die Kommunikation, wenn die Authentifizierung nicht durchgeführt wird.

[0066] Gemäß einem dreiundfünfzigsten Aspekt der vorliegenden Erfindung ermöglicht das Kommunikationsverfahren die Kommunikation zwischen Anschlußeinrichtungen, von denen jede eine Funkkommunikation durch eine gemeinsame Kommunikationsträgersausrüstung ausführen kann und ein Funkkommunikationsnetzwerk nicht durch die gemeinsame Kommunikationsträgersausrüstung in einem Raum bilden kann, in dem Menschen in Mengen, die die Anschlußeinrichtungen tragen, sich sammeln oder vorbeigehen, in dem das Funkkommunikationsnetzwerk unter den Anschlußeinrichtungen gebildet wird, die von mindestens einigen der Menschen getragen werden, selbst wenn ein Bereich, in dem die Funkkommunikation nicht durch die gemeinsame Kommunikationsträger durchgeführt werden kann, in dem Raum vorhanden ist.

[0067] Gemäß einem vierundfünfzigsten Aspekt der vorliegenden Erfindung führen bei dem Kommunikationsverfahren des dreiundfünfzigsten Aspektes einige der Mehrzahl von Anschlußeinrichtungen, die das Funkkommunikations-

netzwerk bilden, die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung durch, wodurch anderen der Anschlußeinrichtungen, die das Funkkommunikationsnetzwerk bilden, ermöglicht wird die Kommunikation durch das Funkkommunikationsnetzwerk und weiter durch die gemeinsame Kommunikationsträgersausrüstung herzustellen.

[0068] Gemäß einem fünfundfünfzigsten Aspekt der vorliegenden Erfindung berechnet bei den Kommunikationsverfahren des dreiundfünfzigsten oder vierundfünfzigsten Aspekt ein paar von Anschlußeinrichtungen, die die gegenseitige Kommunikation durch das Funkkommunikationsnetzwerk durchführen, die einen Teil der Anschlußeinrichtungen darstellen, die das Funkkommunikationsnetzwerk bilden, einen geteilten Schlüssel durch Austauschen von Codes zum Identifizieren von sich selbst und Übertragen eines Kommunikationssignales in einer verschlüsselten Form auf der Grundlage des geteilten Schlüssels zu einander.

[0069] Gemäß einem sechsfundfünfzigsten Aspekt der vorliegenden Erfindung wird bei dem Kommunikationsverfahren nach einem des dreiundfünfzigsten bis fünfundfünfzigsten Aspektes die Kommunikation durch das Funkkommunikationsnetzwerk nur für Notfallkommunikation erlaubt.

[0070] Gemäß einem siebenundfünfzigsten Aspekt der vorliegenden Erfindung wird bei dem Kommunikationsverfahren nach einem des dreiundfünfzigsten bis sechsfundfünfzigsten Aspektes eine andere Anschlußeinrichtung, die das Funkkommunikationsnetzwerk bilden kann, in dem Bereich eingebaut, in dem die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung nicht durchgeführt wird, wodurch die Bildung des Funkkommunikationsnetzwerkes ermöglicht wird, selbst wenn die Bevölkerungsdichte von Personen, die die Anschlußeinrichtungen tragen, niedrig ist.

[0071] Bei der Halbleitervorrichtung des ersten Aspektes der vorliegenden Erfindung kann, da der Code zum Identifizieren des Halbleitersubstrates in einem anderen Halbleitersubstrat gespeichert ist, eine betrügerische Benutzung eines Gerätes, das die vorliegende Erfindung enthält, durch die Ersetzung des Halbleitersubstrates durch Überprüfen dieser Codes verhindert werden.

[0072] Bei der Halbleitervorrichtung des zweiten Aspektes der vorliegenden Erfindung gibt es, da der Code in dem OTPROM des Speichers gespeichert ist, eine hohe Barriere (Sicherheit) gegen betrügerische Änderung des in dem Speicher gespeicherten Codes.

[0073] Bei der Halbleitervorrichtung des dritten Aspektes der vorliegenden Erfindung ist es, da der Identifikationscode durch Benutzen der Variation der elektrischen Eigenschaften der Halbleiterelemente erzeugt wird, möglich, die Halbleiterelemente zu benutzen, die durch den gleichen Vorgang hergestellt sind, aus den vorhandenen Vorrichtungen, die durch Massenproduktion hergestellt sind. Daher kann der Herstellungsvorgang der vorliegenden Vorrichtung vereinfacht werden. Da weiter die elektrische Eigenschaft des Halbleiterelementes, auf der die Identifikationscode ruht, nicht von außen geändert werden kann, gibt es eine hohe Barriere gegen betrügerische Änderung des Identifikationscodes.

[0074] Bei der Halbleitervorrichtung des vierten Aspektes der vorliegenden Erfindung gibt es, da das Halbleiterelement eine polykristalline Substanz aufweist und der Identifikationscode erzeugt wird unter Benutzung der Variation (d. h. Dispersion) der Kristallstruktur der polykristallinen Substanz, eine große Variation der elektrischen Eigenschaft der Halbleiterelemente, die durch den gleichen Vorgang hergestellt sind. Daher ist es leicht, eine Übereinstimmung der

Identifikationscodes unter massenproduzierten vorhandenen Vorrichtung zu verhindern.

[0075] Bei der Halbleitervorrichtung des fünften Aspektes der vorliegenden Erfindung gibt es, da der Identifikationscode in dem OTPROM der Codeerzeugereinheit gespeichert ist, eine hohe Barriere gegen betrügerische Änderung des Identifikationscodes, der von der Codeerzeugereinheit erzeugt wird.

[0076] Bei der Halbleitervorrichtung des sechsten Aspektes der vorliegenden Erfindung ist es, da die Komperatorschaltung die Beurteilung auf die Übereinstimmung der Codes durchführt, möglich, das Freigabesignal für die Authentifizierung zu benutzen.

[0077] Bei der Halbleitervorrichtung des siebten Aspektes der vorliegenden Erfindung ist die Komperatorschaltung in dem Halbleitersubstrat gebildet, in dem die Codeerzeugereinheit gebildet ist, es ist unmöglich, den Identifikationscode betrügerisch zu ändern, der von der Codeerzeugereinheit an die Komperatorschaltung in dem gleichen Halbleitersubstrat eingegeben wird, von der Außenseite. Daher gibt es eine höhere Barriere gegen betrügerische Benutzung.

[0078] Bei der Halbleitervorrichtung des achten Aspektes der vorliegenden Erfindung ist es unmöglich, da die Codes in der Verschlüsselform zwischen verschiedenen Halbleitersubstraten übertragen werden, die Codes von der Außenseite zu lesen. Daher gibt es eine noch höhere Barriere gegen betrügerische Benutzung.

[0079] Bei der Halbleitervorrichtung des neunten Aspektes der Erfindung ist es möglich, da der Schlüssel durch Benutzen der Variation der elektrischen Eigenschaften der Halbleiterelemente erzeugt wird, die Halbleiterelemente zu benutzen, die durch den gleichen Vorgang hergestellt werden, aus einer Menge von vorhandenen massenproduzierten Vorrichtungen. Daher kann der Herstellungsvorgang der vorliegenden Vorrichtung vereinfacht werden. Da weiter die elektrische Eigenschaft des Halbleiterelementes, auf der der Schlüssel beruht, nicht von außen geändert werden kann, gibt es eine hohe Barriere gegen betrügerische Änderung des Schlüssels.

[0080] Bei der Halbleitervorrichtung des zehnten Aspektes der vorliegenden Erfindung gibt es eine große Variation der elektrischen Eigenschaft der Halbleiterelemente, die durch den gleichen Vorgang hergestellt sind, da das Halbleiterelement eine polykristalline Substanz aufweist und der Schlüssel unter Benutzung der Variation (d. h. Dispersion) der Kristallstruktur der polykristallinen Substanz erzeugt wird. Daher ist es leicht eine Übereinstimmung der Schlüssel unter der Menge der massenproduzierten vorhandenen Vorrichtungen zu verhindern.

[0081] Bei der Halbleitervorrichtung des elften Aspektes der vorliegenden Erfindung gibt es eine hohe Barriere gegen eine betrügerische Änderung des Schlüssels, der durch die Schlüsselerzeugereinheit erzeugt ist, da der Schlüssel in dem OTPROM der Schlüsselerzeugereinheit gespeichert ist.

[0082] Da die Halbleitervorrichtung des zwölften Aspektes der vorliegenden Erfindung die Umschalterschaltung aufweist, ist es möglich, eine betrügerische Benutzung durch Eingeben des Identifikationscodes zu verhindern, der von dem Halbleitersubstrat ausgegeben wird, der den Speichercode fälscht, an das gleiche Halbleitersubstrat.

[0083] Da die Halbleitervorrichtung des dreizehnten Aspektes der vorliegenden Erfindung die vorbestimmte Schaltung mit dem Schaltungsabschnitt aufweist, der selektiv in einen aktiven Zustand oder einen inaktiven Zustand kommt in Abhängigkeit der Beurteilung der Komperatorschaltung, ist es möglich, eine vorbestimmte Tätigkeit des Gerätes freizugeben oder zu sperren in Abhängigkeit des Vergleichsresultat, in dem die vorbestimmte Schaltung als

Teil einer Schaltung zum Erzielen der Funktion des Gerätes benutzt wird.

[0084] Bei der Halbleitervorrichtung des vierzehnten Aspektes der vorliegenden Erfindung kann, da die vorbestimmte Schaltung in einem der Halbleitersubstrate gebildet ist, in dem die Codeerzeugereinheit und die Komperatorschaltung gebildet sind, das von der Komperatorschaltung an die vorbestimmte Schaltung in dem gleichen Halbleitersubstrat eingegebene Freigabesignal nicht von außen eingegeben werden. Daher gibt es eine noch höhere Barriere gegen betrügerische Benutzung.

[0085] Die Halbleitervorrichtung des fünfzehnten Aspektes der vorliegenden Erfindung weist die einfachste Struktur auf, bei der die Codeerzeugereinheit in einem der zwei Halbleitersubstrate gebildet ist und der Speicher in dem anderen gebildet ist, und der Code, der mit dem Identifikationscode übereinstimmt, der dem einen der Halbleitersubstrate innewohnt, in dem anderen Halbleitersubstrat gespeichert ist. Daher ist es leicht, die Vorrichtung herzustellen, und möglich, die Größe der Vorrichtung zu verringern.

[0086] Bei der Halbleitervorrichtung des sechzehnten Aspektes der vorliegenden Erfindung sind die Codeerzeugereinheit und der Speicher jeweils in beiden der zwei Halbleitersubstrate gebildet, und die zwei Halbleitersubstrate speichern die Codes die jeweils mit dem Identifikationscode des anderen übereinstimmen, es ist möglich, die Zahl der Halbleitersubstrate auf ein Minimum zu drücken und eine höhere Barriere gegen die betrügerische Benutzung zu erzielen.

[0087] Bei der Anschlußeinrichtung des siebzehnten Aspektes der vorliegenden Erfindung gibt es eine hohe Barriere gegen Lecken von Information, die die Daten darstellt, da die Daten in der verschlüsselten Form zu und von der Außenseite übertragen und empfangen werden. Da weiterhin der Schlüssel für die Verschlüsselung unter Benutzung der Variation der elektrischen Eigenschaften der Halbleiterelemente erzeugt wird, ist es möglich, die Halbleiterelemente zu benutzen, die durch den gleichen Vorgang hergestellt werden, aus einer Menge von massenproduzierten vorhandenen Vorrichtungen. Daher kann der Herstellungsvorgang der vorliegenden Vorrichtung vereinfacht werden. Da weiter die elektrische Eigenschaft des Halbleiterelementes, auf der der Schlüssel beruht, nicht von außen geändert werden kann, gibt es eine hohe Barriere gegen eine betrügerische Änderung des Schlüssels.

[0088] Bei der Anschlußeinrichtung des achtzehnten Aspektes der vorliegenden Erfindung kann, da die Schlüssel erzeugereinheit in dem Hilfsabschnitt eingebaut ist, der von dem Hauptkörperabschnitt abnehmbar ist, ein Schlüssel für eine Mehrzahl von Hauptkörperabschnitten benutzt werden.

[0089] Bei der Anschlußeinrichtung des neunzehnten Aspektes der vorliegenden Erfindung ist, da die Schlüsselerzeugereinheit in der IC-Karte eingebaut ist, sie leicht zu tragen.

[0090] Bei der Anschlußeinrichtung des zwanzigsten Aspektes der vorliegenden Erfindung gibt es, da das Halbleiterelemente eine polykristalline Substanz aufweist und der Schlüssel unter Benutzung der Variation (d. h. Dispersion) der Kristallstrukturen der polykristallinen Substanzen erzeugt wird, eine große Variation der elektrischen Eigenschaft der Halbleiterelemente, die durch den gleichen Vorgang hergestellt werden. Daher ist es leicht eine Übereinstimmung der Schlüssel zu verhindern unter einer Menge von massenproduzierten vorhandenen Vorrichtungen.

[0091] Da die Anschlußeinrichtung des einundzwanzigsten Aspektes der vorliegenden Erfindung die Kommunikationsschaltung aufweist, die mindestens eines von der Übertragung und des Empfanges stoppt, wenn die Beurteilung

der Komperatorschaltung nicht Übereinstimmung anzeigt, ist es möglich, automatisch eine betrügerische Benutzung des Gerätes zu unterdrücken, das die vorliegende Vorrichtung für Kommunikation enthält, durch Ersetzen des Halbleitersubstrates, durch die Wirkung der Anschlußeinrichtung selbst ohne eine Prozedur der gemeinsamen Kommunikationsträgersausrüstung.

[0092] Bei der Anschlußeinrichtung des zweiundzwanzigsten Aspektes der vorliegenden Erfindung führt, da das Freigabesignal übertragen wird, die gemeinsame Kommunikationsträgersausrüstung die Authentifizierung auf der Grundlage des Freigabesignales durch zum Verhindern einer betrügerischen Benutzung des Gerätes, daß die vorliegende Vorrichtung enthält zur Kommunikation, durch Ersetzen des Halbleitersubstrates.

[0093] Bei der Anschlußeinrichtung des dreiundzwanzigsten Aspektes der vorliegenden Erfindung vergleicht, da der Identifikationscode und der Speichercode übertragen werden, die gemeinsame Kommunikationsträgersausrüstung diese Codes und führt die Authentifizierung auf der Grundlage des Vergleichsresultates durch zum Verhindern einer betrügerischen Benutzung des Gerätes, das die vorliegende Vorrichtung zur Kommunikation enthält, durch Ersetzen des Halbleitersubstrates.

[0094] Bei der Anschlußeinrichtung des vierundzwanzigsten Aspektes der vorliegenden Erfindung kann, da der Speicher in dem Hilfsabschnitt eingebaut ist, der von dem Hauptkörperabschnitt abnehmbar ist, die gemeinsame Kommunikationsträgersausrüstung die Authentifizierungen der verschiedenen Niveaus in zwei Fällen ausführen, in denen der Hauptkörperabschnitt und der Hilfsabschnitt kombiniert sind, und in denen der Hauptkörperabschnitt und der Hilfsabschnitt nicht kombiniert sind. Zum Beispiel wird die Hochniveauauthentifizierung durchgeführt, wenn der Hauptkörperabschnitt und der Hilfsabschnitt kombiniert sind, und die gemeinsame Kommunikationsträgersausrüstung kann die Kommunikationsladung für die Kommunikation davor als bestätigt aufzeichnen, und es ist möglich, eine ungesetzliche Tätigkeit des Vermeidens der Pflicht des Zahlens zu verhindern unter dem Vorwand, daß die Anschlußeinrichtung verloren worden ist.

[0095] Bei der Anschlußeinrichtung des fünfundzwanzigsten Aspektes der vorliegenden Erfindung gibt es, da der Identifikationscode und der Speichercode in der verschlüsselten Form übertragen werden, eine hohe Barriere gegen Lecken des Codes.

[0096] Bei der Speichereinrichtung des sechsundzwanzigsten Aspektes der vorliegenden Erfindung gibt es, da die erste Schlüsselerzeugereinheit und die erste Verschlüsselungsschaltung in einem einzigen Halbleitersubstrat zusammen mit der Codeerzeugereinheit gebildet sind, eine höhere Barriere gegen das Lecken des Identifikationscodes und des ersten Schlüssels.

[0097] Bei der Anschlußeinrichtung des siebenundzwanzigsten Aspektes der vorliegenden Erfindung gibt es, da die zweite Schlüsselerzeugereinheit und die zweite Verschlüsselungsschaltung in einem einzigen Halbleitersubstrat zusammen mit dem Speicher gebildet sind, eine höhere Barriere gegen das Lecken des Speicher codes und des zweiten Schlüssels.

[0098] Bei der Anschlußeinrichtung des achtundzwanzigsten Aspektes der vorliegenden Erfindung sind, da der Hilfsabschnitt das Batterieladegerät ist, das die Batterie des Hauptkörperabschnittes auflädt, der Hauptkörperabschnitt und der Hilfsabschnitt periodisch miteinander verbunden ohne eine extra Arbeit des Benutzers.

[0099] Bei der Anschlußeinrichtung des neunundzwanzigsten Aspektes der vorliegenden Erfindung ist es, da der

Hilfsabschnitt die IC-Karte ist, leicht zu tragen. Da weiter die Codes zwischen dem Hauptkörperabschnitt und dem Hilfsabschnitt drahtlos übertragen werden, ist es möglich, die Kombination des Hauptkörperabschnittes und des Hilfsabschnittes nur durch Tragen der IC-Karte und des Hauptkörperabschnittes zu erzielen.

[0100] Bei der Anschlußeinrichtung des dreißigsten Aspektes der vorliegenden Erfindung können, da die Kommunikationsschaltung in einem der Halbleitersubstrate gebildet ist, in der die Codeerzeugereinheit gebildet ist, das Freigabesignal oder die Codes, die an die Kommunikationsschaltung in dem gleichen Halbleitersubstrat eingegeben werden, nicht von der Außenseite eingegeben werden. Daher gibt es eine höhere Barriere gegen die betrügerische Benutzung.

[0101] Bei der Anschlußeinrichtung des einunddreißigsten Aspektes der vorliegenden Erfindung kann die Kommunikation in dem Raum hergestellt werden, in dem Menschen in Mengen, die die Anschlußeinrichtungen tragen, sich sammeln oder vorbeigehen, in dem das Funkkommunikationsnetzwerk unter den Anschlußeinrichtungen gebildet wird, die von mindestens einigen der Leuten getragen werden, selbst wenn der Bereich, in dem die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung nicht ausgeführt werden kann, zum Beispiel in einem unterirdischen Einkaufsgebiet, in dem Raum vorhanden ist.

[0102] Da die Anschlußeinrichtung des zweiunddreißigsten Aspektes der vorliegenden Erfindung die Selektorschaltung aufweist kann durch die Anschlußeinrichtung die Kommunikation zwischen anderen Personen, die nicht der Benutzer der Anschlußeinrichtung sind, durch das Funkkommunikationsnetzwerk übertragen, sondern auch der Benutzer der Anschlußeinrichtung kann die Kommunikation durch das Funkkommunikationsnetzwerk durchführen.

[0103] Bei der Anschlußeinrichtung des dreiunddreißigsten Aspektes der vorliegenden Erfindung gibt es, da der gemeinsame Schlüssel eingestellt werden kann durch Austausch der Codes mit dem Kommunikationspartner und das Kommunikationssignal in der verschlüsselten Form auf der Grundlage des geteilten Schlüssels übertragen wird, eine hohe Barriere gegen das Lecken des Inhaltes der Kommunikation mit irgendeinem Kommunikationspartner.

[0104] Bei der Anschlußeinrichtung des vierunddreißigsten Aspektes der vorliegenden Erfindung ist es, da der Code, auf dem der geteilte Schlüssel basiert, benutzt wird unter Benutzung der Variation der elektrischen Eigenschaften der Halbleiterelemente erzeugt wird, möglich, die Halbleiterelemente zu benutzen, die durch den gleichen Vorgang aus einer Menge von massenproduzierten vorhandenen Vorrichtungen hergestellt sind. Daher kann der Herstellungsvorgang der vorliegenden Vorrichtung vereinfacht werden. Da weiter die elektrische Eigenschaft des Halbleiterelementes, auf der der Code beruht, nicht von außen geändert werden kann, gibt es eine hohe Barriere gegen die betrügerische Änderung des Codes.

[0105] Bei der Anschlußeinrichtung des fünfunddreißigsten Aspektes der vorliegenden Erfindung gibt es, da das Halbleiterelement eine polykristalline Substanz aufweist und der Code erzeugt wird durch Benutzen der Variation (d. h. Dispersion) der Kristallstruktur der polykristallinen Substanz, eine große Variation in der elektrischen Eigenschaft der Halbleiterelemente, die durch den gleichen Vorgang hergestellt sind. Daher ist es leicht, Übereinstimmung dieser Codes unter einer Menge von massenproduzierten vorliegenden Vorrichtungen zu vermeiden.

[0106] Bei der Anschlußeinrichtung des sechsunddreißigsten Aspektes der vorliegenden Erfindung gibt es, da der Code in dem OTPROM der Codeerzeugereinheit gespeichert

ist, eine hohe Barriere gegen eine betrügerische Änderung des durch die Codeerzeugereinheit erzeugten Codes.

[0107] Bei der Anschlußeinrichtung des siebenunddreißigsten Aspektes der vorliegenden Erfindung ist es, da das von der Funkkommunikationsnetzwerkschaltung empfangene Signal zu der Kommunikationsschaltung übertragen wird, nachdem es demoduliert und dann moduliert wird, möglich, das Benutzungsverhältnis des Frequenzbandes der Kommunikationsschaltung zu verbessern.

[0108] Bei dem Kommunikationsverfahren des achtunddreißigsten Aspektes der vorliegenden Erfindung ist es, da das Freigabesignal, das von der Anschlußeinrichtung übertragen wird, zur Authentifizierung benutzt wird, möglich, eine betrügerische Benutzung des Gerätes durch Ersetzen des Halbleitersubstrates zu verhindern, das die vorliegende Einrichtung zur Kommunikation enthält.

[0109] Bei dem Kommunikationsverfahren des neununddreißigsten Aspektes der vorliegenden Erfindung ist es, da der Identifikationscode und der Speichercode, die von der Anschlußeinrichtung übertragen werden, für die Authentifizierung benutzt werden, möglich, eine betrügerische Benutzung des Gerätes durch Ersetzen des Halbleitersubstrates zu verhindern, das die vorliegende Einrichtung zur Kommunikation enthält.

[0110] Bei dem Kommunikationsverfahren des vierzigsten Aspektes der vorliegenden Erfindung ist es, da der Identifikationscode und der Speichercode, die empfangen werden, aufgezeichnet werden, möglich, wirksam ein Verbrechen zu unterdrücken mit der betrügerischen Benutzung, bevor es ausgeführt wird. Weiter kann, wenn die betrügerische Benutzung durchgeführt wird, der aufgezeichnete Code nützlich sein zum Spezifizieren des unautorisierten Benutzers.

[0111] Bei dem Kommunikationsverfahren des einundvierzigsten Aspektes der vorliegenden Erfindung kann, da der Identifikationscode und der Speichercode, die empfangen werden, aufgezeichnet werden, wenn die Authentifizierung nicht in dem Authentifizierungsschritt durchgeführt wird, d. h. wenn der Benutzer nicht autorisiert ist, die aufgezeichneten Codes nützlich sein zum Spezifizieren des unautorisierten Benutzers.

[0112] Bei dem Kommunikationsverfahren des zweiundvierzigsten Aspektes der vorliegenden Erfindung werden Authentifizierungen verschiedener Niveaus in zwei Fällen durchgeführt, in dem der Hauptkörperabschnitt und der Hilfsabschnitt kombiniert sind, und in dem der Hauptkörperabschnitt und der Hilfsabschnitt nicht kombiniert sind. Da die Hochniveauintifizierung in Kombination mit dem Hauptkörperabschnitt und dem Hilfsabschnitt nur durchgeführt wird, wenn sowohl der Identifikationscode als auch der Speichercode mit den registrierten Codes übereinstimmen, beweist die Hochniveauintifizierung, daß die Anschlußeinrichtung gültig benutzt wird, mit höherer Genauigkeit. Daher kann die gemeinsame Kommunikationsträgersausrüstung selektiv die zwei Authentifizierungen gemäß der Wichtigkeit der Prozedur benutzen.

[0113] Bei dem Kommunikationsverfahren des dreiundvierzigsten Aspektes der vorliegenden Erfindung muß nur, da der zu registrierende Speichercode zu der gemeinsamen Kommunikationsträgersausrüstung durch Ausführen der Kommunikation mit dem Hilfsabschnitt übertragen wird, der an dem Hauptkörperabschnitt angebracht ist, der Identifizierungscode registriert werden, bevor die Anschlußeinrichtung an den Benutzer geliefert wird.

[0114] Bei dem Kommunikationsverfahren des vierundvierzigsten Aspektes der vorliegenden Erfindung kann, da der zweite registrierte Code geändert werden kann, der Benutzer den Hilfsabschnitt ändern, falls es nötig ist, nachdem

Erhalt der Anschlußeinrichtung.

[0115] Bei dem Kommunikationsverfahren des fünfundvierzigsten Aspektes der vorliegenden Erfindung werden die Authentifizierungen auf verschiedenen Niveaus in zwei Fällen durchgeführt, in dem der Hauptkörperabschnitt und der Hilfsabschnitt kombiniert sind, und in dem der Hauptkörperabschnitt und der Hilfsabschnitt nicht kombiniert sind. Da die Hochniveauauthentifizierung in Kombination mit dem Hauptkörperabschnitt und dem Hilfsabschnitt nur durchgeführt wird, wenn sowohl der Identifikationscode als auch der Speichercode mit den registrierten Codes übereinstimmen, beweist die Hochniveauauthentifizierung, daß die Anschlußeinrichtung gültig benutzt wird, mit höherer Genauigkeit. Daher kann die gemeinsame Kommunikationsträgersausrüstung selektiv die zwei Authentifizierungen gemäß der Wichtigkeit der Prozedur benutzen. Da weiter der Identifikationscode und der Speichercode in der verschlüsselten Form übertragen werden, gibt es eine hohe Barriere gegen das Lecken der Codes.

[0116] Bei dem Kommunikationsverfahren des sechsundvierzigsten Aspektes der vorliegenden Erfindung braucht nur, da der zu registrierende Speichercode zu der gemeinsamen Kommunikationsträgersausrüstung durch Durchführen der Kommunikation mit dem an dem Hauptkörperabschnitt angebrachten Hilfsabschnitt übertragen wird, der Identifikationscode registriert zu werden, bevor die Anschlußeinrichtung an den Benutzer geliefert wird.

[0117] Bei dem Kommunikationsverfahren des siebenundvierzigsten Aspektes der vorliegenden Erfindung kann, da der zweite registrierte Code geändert werden kann, der Benutzer den Hilfsabschnitt ändern, falls es nötig ist, nachdem die Anschlußeinrichtung erhalten ist.

[0118] Bei dem Kommunikationsverfahren des achtundvierzigsten Aspektes der vorliegenden Erfindung können, da der Identifikationscode und der Speichercode, die empfangen werden, aufgezeichnet werden, wenn die Hochniveauauthentifizierung in dem Hochniveauauthentifizierungsschritt nicht durchgeführt wird, d. h. wenn es eine starke Möglichkeit gibt, daß der Benutzer nicht autorisiert ist, die aufgezeichneten Codes nützlich zum Spezifizieren des unautorisierten Benutzers seien.

[0119] Bei dem Kommunikationsverfahren des neunundvierzigsten Aspektes der vorliegenden Erfindung ist es möglich, da die Kommunikationsladung für die Kommunikation zuvor aufgezeichnet wird, wie sie bestätigt wird, wenn die Hochniveauauthentifizierung in dem Hochniveauauthentifizierungsschritt durchgeführt wird, d. h. wenn es eine starke Möglichkeit gibt, daß der Benutzer autorisiert ist, eine illegale Tätigkeit des Vermeidens der Pflicht des Zahlens zu verhindern unter dem Vorwand, daß die Anschlußeinrichtung verloren worden ist.

[0120] Bei dem Kommunikationsverfahren des fünfzigsten Aspektes der vorliegenden Erfindung ist es möglich, da das Beurteilungsergebnis, das in dem Hochniveauauthentifizierungsschritt gemacht wurde, auf der normalen Authentifizierung wiedergegeben wird, die durchgeführt wird, wenn der Hilfsabschnitt nicht an dem Hauptkörperabschnitt angebracht ist, eine wichtige Prozedur wie eine Geschäftstätigkeit unter der normalen Authentifizierung durchzuführen.

[0121] Bei dem Kommunikationsverfahren des einundfünfzigsten Aspektes der vorliegenden Erfindung ist es möglich, da, ob die Geschäftstätigkeit durch die Kommunikation davor ausgeführt ist oder nicht, aufgezeichnet ist gemäß dem, ob die Hochniveauauthentifikation in dem Hochniveauauthentifikationsschritt durchgeführt ist oder nicht, den Verlust durch illegale Geschäftstätigkeiten auf der Grundlage der betrügerischen Benutzung der Anschlußeinrichtung zu lösen oder zu verringern.

[0122] Bei dem Kommunikationsverfahren des zweiundfünfzigsten Aspektes der vorliegenden Erfindung ist es möglich, da die Kommunikation gemäß dessen fortgesetzt wird oder gestoppt wird, ob die Authentifizierung in dem Authentifizierungsschritt durchgeführt oder nicht ist, die Kommunikation auf der Grundlage der betrügerischen Benutzung der Anschlußeinrichtung zu verhindern.

[0123] Bei dem Kommunikationsverfahren des dreiundfünfzigsten Aspektes der vorliegenden Erfindung kann die Kommunikation in einem Raum hergestellt werden, in dem Leute in Mengen, die die Anschlußeinrichtungen mit der vorbestimmten Funktion tragen, durch Sammeln oder Vorbeigehen, in dem das Funkkommunikationsnetzwerk unter den Anschlußeinrichtungen gebildet wird, die von mindestens einigen der Leuten getragen werden, selbst wenn der Bereich, in dem die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung nicht ausgeführt werden kann, d. h. in einem unterirdischen Einkaufsgebiet, in dem Raum vorhanden ist.

[0124] Bei dem Kommunikationsverfahren des vierundfünfzigsten Aspektes der vorliegenden Erfindung wird es möglich, da einige der Anschlußeinrichtungen, die das Funkkommunikationsnetzwerk bilden, die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung durchführen zum Ermöglichen, daß andere der Anschlußeinrichtungen die Kommunikation durch das Funkkommunikationsnetzwerk und weiter durch die gemeinsame Kommunikationsträgersausrüstung durchführen, die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung von dem Bereich herzustellen, indem die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung nicht durchgeführt werden kann, z. B. in einem unterirdischen Einkaufsgebiet.

[0125] Bei dem Kommunikationsverfahren des fünfundfünfzigsten Aspektes der vorliegenden Erfindung gibt es, da der gemeinsame Schlüssel durch Austauschen der Codes mit dem Kommunikationspartner eingestellt wird und das Kommunikationssignal in verschlüsselter Form auf der Grundlage des geteilten Schlüssels übertragen wird, eine hohe Barriere gegen Lecken des Inhaltes der Kommunikation mit irgendeinem Kommunikationspartner.

[0126] Bei dem Kommunikationsverfahren des sechsundfünfzigsten Aspektes der vorliegenden Erfindung, da die Kommunikation durch das Funkkommunikationsnetzwerk nur in Notfallkommunikation erlaubt ist, wie eine Anforderung zur Hilfe zu einer Zeit, an der ein Notfall auftritt, der Leben und Eigentum bedroht, braucht dieses nicht der Vorgang zum Verschlüsseln zum Verhindern des Leckens des Inhaltes der Kommunikation zu sein.

[0127] Bei dem Kommunikationsverfahren des siebenundfünfzigsten Aspektes der vorliegenden Erfindung kann, da die Anschlußeinrichtung, die das Funkkommunikationsnetzwerk bilden kann, in dem Bereich eingebaut ist, in dem die Funkverbindung durch die gemeinsame Kommunikationsträgersausrüstung nicht ausgeführt werden kann, z. B. in einer unterirdischen Einkaufsgegend, die Kommunikation durch das Funkkommunikationsnetzwerk hergestellt werden, selbst wenn die Populationsdichte der Person, die die Anschlußeinrichtung mit der vorbestimmten Funktion tragen, in dem Bereich niedrig ist.

[0128] Andere Merkmale und Zweckmäßigkeiten der Erfindung werden ersichtlicher aus der folgenden Beschreibung von Ausführungsformen anhand der Figuren. Von den Figuren zeigen:

[0129] Fig. 1 ein Blockschaltbild, das eine Halbleitervorrichtung gemäß einer ersten Ausführungsform der vorliegenden Erfindung zeigt;

[0130] Fig. 2 ein Blockschaltbild, das eine Codeerzeuger-

einheit von Fig. 1 zeigt;

[0131] Fig. 3 eine Draufsicht, die ein Halbleiterelement von Fig. 2 zeigt;

[0132] Fig. 4 ein Querschnitt, der entlang der Linie A-A des Halbleiterelementes von Fig. 3 genommen ist;

[0133] Fig. 5 eine Draufsicht, die ein Halbleiterelement von Fig. 2 zeigt;

[0134] Fig. 6 ein Diagramm, das die Eigenschaften des Halbleiterelementes von Fig. 2 darstellt;

[0135] Fig. 7 ein Blockschaltbild, das ein anderes Beispiel der Codeerzeugereinheit von Fig. 1 zeigt;

[0136] Fig. 8 ein Blockschaltbild, das einen Speicher von Fig. 1 zeigt;

[0137] Fig. 9 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß der ersten Ausführungsform der vorliegenden Erfindung zeigt;

[0138] Fig. 10 ein Blockschaltbild, das eine Kommunikationsschaltung von Fig. 9 zeigt;

[0139] Fig. 11 ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung von Fig. 9;

[0140] Fig. 12 ein Blockschaltbild, das ein Kommunikationssystem gemäß der ersten Ausführungsform der vorliegenden Erfindung zeigt;

[0141] Fig. 13 ein Blockschaltbild, das eine Halbleitervorrichtung gemäß einer zweiten Ausführungsform der vorliegenden Erfindung zeigt;

[0142] Fig. 14 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß der zweiten Ausführungsform der vorliegenden Erfindung zeigt;

[0143] Fig. 15 ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung von Fig. 13;

[0144] Fig. 16 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß einer dritten Ausführungsform der vorliegenden Erfindung zeigt;

[0145] Fig. 17 ein Flußdiagramm eines Kommunikationsverfahrens, das die Anschlußeinrichtung von Fig. 16 benutzt;

[0146] Fig. 18 ein Blockschaltbild, das ein anderes Beispiel der Anschlußeinrichtung gemäß der dritten Ausführungsform der vorliegenden Erfindung zeigt;

[0147] Fig. 19 ein Flußdiagramm eines Kommunikationsverfahrens, das die Anschlußeinrichtung von Fig. 18 benutzt;

[0148] Fig. 20 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß einer vierten Ausführungsform der vorliegenden Erfindung zeigt;

[0149] Fig. 21 ein Flußdiagramm des Kommunikationsverfahrens, das die Anschlußeinrichtung von Fig. 20 benutzt;

[0150] Fig. 22 ein Blockschaltbild, das ein anderes Beispiel der Anschlußeinrichtung gemäß der vierten Ausführungsform der vorliegenden Erfindung zeigt;

[0151] Fig. 23 ein Flußdiagramm des Kommunikationsverfahrens, das die Anschlußeinrichtung von Fig. 22 benutzt;

[0152] Fig. 24 ein Blockschaltbild, das eine Halbleitervorrichtung gemäß einer fünften Ausführungsform der vorliegenden Erfindung zeigt;

[0153] Fig. 25 ein Blockschaltbild, das eine Schlüsselerzeugereinheit von Fig. 24 zeigt;

[0154] Fig. 26 ein Blockschaltbild, das ein anderes Beispiel der Schlüsselerzeugereinheit von Fig. 24 zeigt;

[0155] Fig. 27 ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung, die die Halbleitervorrichtung von Fig. 24 enthält;

[0156] Fig. 28 ein Blockschaltbild, das ein anderes Beispiel der Halbleitervorrichtung gemäß der fünften Ausführungsform der vorliegenden Erfindung zeigt;

[0157] Fig. 29 ein Flußdiagramm einer Prozedur zur Benutzung der Anschlußeinrichtung, die die Halbleitervorrich-

tung von Fig. 28 enthält;

[0158] Fig. 30 ein Blockschaltbild einer Halbleitervorrichtung gemäß einer sechsten Ausführungsform der vorliegenden Erfindung;

5 [0159] Fig. 31 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß einer siebten Ausführungsform der vorliegenden Erfindung zeigt;

[0160] Fig. 32 ein Blockschaltbild, das ein anderes Beispiel der Anschlußeinrichtung gemäß der siebten Ausführungsform der vorliegenden Erfindung zeigt;

10 [0161] Fig. 33 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß einer achten Ausführungsform der vorliegenden Erfindung zeigt;

[0162] Fig. 34 ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung von Fig. 33;

15 [0163] Fig. 35 u. 36 Flußdiagramme des Schrittes S509 von Fig. 34;

[0164] Fig. 37 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß einer neunten Ausführungsform der vorliegenden Erfindung zeigt;

20 [0165] Fig. 38 ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung von Fig. 37;

[0166] Fig. 39 u. 40 Flußdiagramme des Schrittes S709 von Fig. 38;

25 [0167] Fig. 41 ein Flußdiagramm eines anderen Beispiels des Schrittes S709 von Fig. 38;

[0168] Fig. 42 u. 43 Flußdiagramme des Schrittes S742 von Fig. 41;

[0169] Fig. 44 u. 45 Flußdiagramme eines anderen Beispiels des Schrittes S709 von Fig. 38;

30 [0170] Fig. 46 ein Blockschaltbild, das ein anderes Beispiel der Anschlußeinrichtung gemäß der neunten Ausführungsform der vorliegenden Erfindung zeigt;

[0171] Fig. 47 ein erläuterndes Bild eines Kommunikationsverfahrens gemäß einer zehnten Ausführungsform der vorliegenden Erfindung;

[0172] Fig. 48 ein Blockschaltbild, das eine Anschlußeinrichtung gemäß der zehnten Ausführungsform der vorliegenden Erfindung zeigt;

40 [0173] Fig. 49 ein Blockschaltbild, das ein anderes Beispiel der Anschlußeinrichtung gemäß der zehnten Ausführungsform der vorliegenden Erfindung zeigt;

[0174] Fig. 50 ein Blockschaltbild, das eine Schlüsselerzeugereinheit von Fig. 49 zeigt;

45 [0175] Fig. 51 ein Flußdiagramm der Schlüsselerzeugung durch die Anschlußeinrichtung von Fig. 49;

[0176] Fig. 52 ein Blockschaltbild, das ein noch anderes Beispiel der Anschlußeinrichtung gemäß der zehnten Ausführungsform der vorliegenden Erfindung zeigt;

50 [0177] Fig. 53 eine Darstellung zum Erläutern eines Betriebes der Anschlußeinrichtung von Fig. 52;

[0178] Fig. 54 eine Darstellung zum Erläutern eines Betriebes im Vergleich mit dem der Fig. 53;

55 [0179] Fig. 55 ein erläuterndes Bild eines anderen Beispiels des Kommunikationsverfahrens gemäß der zehnten Ausführungsform der vorliegenden Erfindung;

[0180] Fig. 56 ein erläuterndes Bild eines Kommunikationsverfahrens gemäß einer elften Ausführungsform der vorliegenden Erfindung;

60 [0181] Fig. 57 ein Schaltbild, das ein Halbleiterelement gemäß einer zwölften Ausführungsform der vorliegenden Erfindung zeigt;

[0182] Fig. 58 eine Darstellung zum Erläutern eines Betriebes des Halbleiterelementes von Fig. 57;

65 [0183] Fig. 59 ein Blockschaltbild, das eine Halbleitervorrichtung gemäß der zwölften Ausführungsform der vorliegenden Erfindung zeigt;

[0184] Fig. 60 ein Schaltbild, das einen Teil der Codier-

schaltung von Fig. 59 zeigt;

[0185] Fig. 61 ein Schaltbild, das ein anderes Beispiel des Halbleiterelementes gemäß der zwölften Ausführungsform der vorliegenden Erfindung zeigt;

[0186] Fig. 62 ein Schaltbild, das ein noch anderes Beispiel des Halbleiterelementes gemäß der zwölften Ausführungsform der vorliegenden Erfindung zeigt;

[0187] Fig. 63 ein Blockschaltbild, das eine Komperatorschaltung des Halbleiterelementes gemäß der zwölften Ausführungsform der vorliegenden Erfindung zeigt;

[0188] Fig. 64 eine Darstellung zum Erläutern der Prozedur eines Kommunikationssystems; und

[0189] Fig. 65 ein Blockschaltbild, das einen Kommunikationsanschluß zeigt.

[0190] Zuerst wird eine Erläuterung eines Ausdruckes gegeben, der in der vorliegenden Beschreibung benutzt wird. In der vorliegenden Beschreibung ist "Übereinstimmung" nicht auf vollständige oder wörtliche Übereinstimmung beschränkt, sondern der Begriff umfaßt auch eine Annäherung in einem vorbestimmten Bereich.

1. Erste Ausführungsform

[0191] Für die erste Ausführungsform wird die Beschreibung über eine Halbleitervorrichtung mit einem Aufbau gegeben, bei dem ein Identifikationscode, der einem von zwei Halbleitersubstraten innewohnt/inhärent ist, in dem anderen der zwei Halbleitersubstrate gespeichert ist, was es möglich macht, eine betrügerische Benutzung durch Ersetzen des Halbleitersubstrates zu verhindern. Die Beschreibung wird auch über eine Anschlußeinrichtung als ein Gerät der Halbleitervorrichtung gegeben.

1.1. Halbleitervorrichtung

[0192] Fig. 1 ist ein Blockschaltbild, das einen Aufbau einer Halbleitervorrichtung gemäß der ersten Ausführungsform der vorliegenden Erfindung zeigt. Diese Halbleitervorrichtung 600 weist eine Codeerzeugereinheit 400, eine Komperatorschaltung 403, eine vorbestimmte Schaltung 405 und einen Speicher 601 auf. Die Codeerzeugereinheit 400, die Komperatorschaltung 403 und die vorbestimmte Schaltung 405 sind in einem Halbleitersubstrat CH1 gebildet, und der Speicher 601 ist in einem anderen Halbleitersubstrat CH2 gebildet. Die Halbleitersubstrate CH1 und CH2 können entweder eingegossene oder nackte Chips sein, die auf einer einzelnen Leiterplatte oder einer Mehrzahl von Leiterplatten angebracht sind.

[0193] Die Codeerzeugereinheit 400 erzeugt einen Identifikationscode Cd, der dem Halbleitersubstrat CH1 inhärent ist/ihm innewohnt. Der Speicher 601 speichert den Identifikationscode Cd, der von der Codeerzeugereinheit 400 erzeugt ist, als einen Speichercode Co. Der Identifikationscode Cd wird von der Codeerzeugereinheit 400 an den Speicher 601 übertragen und in den Speicher 601 geschrieben, bevor die Halbleitervorrichtung 600 als Produkt versendet wird.

[0194] Die Komperatorschaltung 403 vergleicht den Identifikationscode Cd, der von der Codeerzeugereinheit 400 erzeugt wird, mit dem Speichercode Co, der aus dem Speicher 601 gelesen ist, sie beurteilt ob diese Codes miteinander übereinstimmen oder nicht und gibt ein Freigabesignal (oder ein Beurteilungssignal) En aus, das das Beurteilungsergebnis darstellt. Zum Beurteilen der vollständigen Übereinstimmung kann die Komperatorschaltung 403 eine herkömmliche gut bekannte Komperatoreinrichtung sein, die beurteilt, ob die Differenz zwischen den zwei Codes Null ist oder nicht. Zum Erzielen einer Annäherung innerhalb eines vor-

bestimmten Bereiches braucht die Komperatorschaltung 403 nur die Größe der Differenz dieser Codes mit einem vorbestimmten Referenzwert zu vergleichen. Die Größe der Differenz kann durch einen numerischen Wert der Differenz oder die Zahl von Bit geschätzt werden, die sich zwischen den zwei Codes unterscheiden. Weiterhin kann es einen Aufbau der Halbleitervorrichtung 600 geben, bei dem der Referenzwert von außen eingegeben werden kann, und ein Benutzer der Halbleitervorrichtung 600 kann den Referenzwert auf einen gewünschten Wert setzen.

[0195] Die vorbestimmte Schaltung 405 besteht aus einer Mehrzahl von Schaltungselementen zum Erzielen einer vorbestimmten Funktion und enthält einen Schaltungsabschnitt, der selektiv in einen aktiven Zustand oder in einen inaktiven Zustand auf der Grundlage des von der Komperatorschaltung 403 ausgegebenen Freigabesignales En kommt. Die Kommunikationsschaltung 907 von Fig. 65 ist ein Beispiel der vorbestimmten Schaltung 405.

[0196] Bei der Halbleitervorrichtung 600 nach dem obigen Aufbau werden nur, wenn der von der Codeerzeugereinheit 400 erzeugte Identifikationscode Cd und der aus dem Speicher 601 gelesene Speichercode Co miteinander übereinstimmen, alle Abschnitte der vorbestimmten Schaltung 405 tätig. Daher ist es durch Benutzen der vorbestimmten Schaltung 405 als Teil der Schaltungen zum Erzielen der Funktionen eines Gerätes möglich, einen vorbestimmten Betrieb des Gerätes freizugeben oder zu sperren. Wenn es gewollt wird, daß das Halbleitersubstrat CH1 oder CH2 durch ein anderes Halbleitersubstrat zur betrügerischen Benutzung des Gerätes auszutauschen, kann das Gerät einen vorbestimmten Betrieb nicht ausführen, da der Identifikationscode Cd und der Speichercode Co nicht miteinander übereinstimmen.

[0197] Somit kann die betrügerische Benutzung des Gerätes, das die Halbleitervorrichtung 600 enthält, durch Ersetzen des Halbleitersubstrates verhindert werden.

[0198] Es kann einen anderen Aufbau geben, bei dem die Codeerzeugereinheit 400 und die Komperatorschaltung 403 in einem einzigen Halbleitersubstrat CH3 gebildet sind und die vorbestimmte Schaltung 405 in einem anderen Halbleitersubstrat gebildet ist. Bei dem Aufbau, bei dem die vorbestimmte Schaltung 405 in dem einzigen Halbleitersubstrat CH1 zusammen mit der Codeerzeugereinheit 400 und der Komperatorschaltung 403 gebildet ist, kann jedoch das von der Komperatorschaltung 403 an die vorbestimmte Schaltung 405 eingegebene Freigabesignal En nicht von außen eingegeben werden. Daher ist die Barriere (Sicherheit) gegen die betrügerische Benutzung vorteilhafterweise noch höher.

[0199] Weiter kann es einen noch anderen Aufbau geben, bei dem die Komperatorschaltung 403 in einem Halbleitersubstrat gebildet ist, das nicht das Halbleitersubstrat ist, in dem die Codeerzeugereinheit 400 gebildet ist. Bei dem Aufbau, bei dem die Komperatorschaltung 403 in dem Signalhalbleitersubstrat CH1 oder CH3 zusammen mit der Codeerzeugereinheit 400 gebildet ist, kann jedoch der von der Codeerzeugereinheit 400 an die Komperatorschaltung 403 eingegebene Identifikationscode Cd nicht betrügerisch von außen geändert werden. Daher wird die Barriere gegen die betrügerische Benutzung vorteilhafterweise noch höher.

[0200] Weiter kann es einen noch anderen Aufbau geben, bei dem die Halbleitervorrichtung 600 nicht die vorbestimmte Schaltung 405 aufweist. In diesem Fall braucht die vorbestimmte Schaltung 405 nur in dem Gerät getrennt von der Halbleitervorrichtung 600 gebildet zu sein. Alternativ kann es einen anderen Aufbau des Gerätes geben, bei dem das Freigabesignal En aus dem Gerät herausgenommen wird und der aktive/inaktive Zustand des Gerätes von außen ge-

mäß dem Wert des Freigabesignales En gesteuert wird. Eine Anschlußeinrichtung der späteren beschriebenen dritten Ausführungsform ist ein Beispiel dieser Art von Gerät.

[0201] Weiterhin kann es einen Aufbau geben, bei dem die Halbleitervorrichtung 600 weder die vorbestimmte Schaltung 405 noch die Komperatorschaltung 403 aufweist. In diesem Fall müssen die vorbestimmte Schaltung 405 und die Komperatorschaltung 403 nur in dem Gerät getrennt von der Halbleitervorrichtung 600 gebildet werden. Alternativ kann es einen noch anderen Aufbau des Gerätes geben, bei dem der Identifikationscode Cd und der Speichercode Co aus dem Gerät herausgeführt werden und der aktive/inaktive Zustand des Gerätes von außen gemäß den Werten des Identifikationscodes Cd und des Speichercode Co gesteuert wird. Eine Anschlußeinrichtung der später beschriebenen vierten Ausführungsform ist ein Beispiel dieser Art von Gerät.

1.2. Codeerzeugereinheit

[0202] Fig. 2 ist ein Blockschaltbild, das einen internen Aufbau der Codeerzeugereinheit 400 zeigt. Bei dem Beispiel von Fig. 2 weist die Codeerzeugereinheit 400 ein Halbleiterelement 401 und eine Codierschaltung 402 auf. Die Codierschaltung 402 liest die elektrische Eigenschaft des Halbleiterelementes 401 als ein Analogsignal An und wandelt es in ein digitales Signal um. Das durch die Umwandlung erhaltene digitale Signal wird als der Identifikationscode Cd ausgegeben.

[0203] Als die elektrisch Eigenschaft des Halbleiterelementes 401 wird eine Eigenschaft gewählt, die von einem Halbleiterelement 401 zu einem anderen variiert. Der Identifikationscode Cd, der als ein Wert erzeugt wird, der von einem Halbleiterelement 401 zu einem anderen variiert, ist dem Halbleitersubstrat innewohnend/inhärent, in dem die Codeerzeugereinheit 400 gebildet ist. Da die Halbleiterelemente 401, die durch den gleichen Vorgang hergestellt werden, unter einer Menge von Massenproduzierten Halbleitervorrichtungen 600 benutzt werden können, kann der Herstellungsvorgang der Halbleitervorrichtung 600 vereinfacht werden. Da weiter die elektrische Eigenschaft des Halbleiterelementes 401, auf der der Identifikationscode Cd beruht, nicht von der Außenseite geändert werden, ist die Barriere gegen die betrügerische Änderung des Identifikationscodes Cd vorteilhafterweise hoch.

[0204] Das Halbleiterelement 401 weist zum Beispiel eine polykristalline Substanz auf, und eine Eigenschaft die variiert (d. h. dispergiert) mit der Variation (d. h. Dispersion) in den Kristallstrukturen der polykristallinen Substanzen, kann es als die elektrische Eigenschaft benutzt werden. Dieses Beispiel wird später unter Bezugnahme auf Fig. 3 bis 6 beschrieben. Weiter weist das Halbleiterelement 401 zum Beispiel einen MOSFET auf, und die Variation der Schwellenwerte, die durch eine Variation der Dotierungskonzentrationen der Dotierungsdiffusionsbereiche verursacht wird, kann benutzt werden.

[0205] Fig. 3 ist eine Draufsicht, die ein Beispiel des Halbleiterelementes 401 zeigt. Fig. 4 ist ein entlang der Linie A-A von Fig. 3 genommener Querschnitt. Bei diesem Beispiel weist das Halbleiterelement 401 einen Dünnschichttransistor (hier im folgenden als TFT abgekürzt) 101 auf, und eine Halbleiterschicht 1060 mit einem Kanalbereich des TFT 101 ist als eine polykristalline Substanz gebildet. Obwohl weiter eine Halbleiterschicht 1, die als ein Zwischenschritt bei dem Herstellungsverfahren des Halbleiterelementes 401 gebildet ist, zur leichten Darstellung gezeigt ist, wird die Halbleiterschicht 1 selektiv bei dem Herstellungsvorgang geätzt, wobei sie in die Halbleiterschicht 1060 in dem

Halbleiterelement 401 als fertiges Produkt bemustert wird. [0206] Bei dem TFT 101 ist eine Gateelektrode 11 selektiv auf einem Isolierfilm 12 gebildet, und eine Gesamtoberfläche des Isolierfilm 12 und der Gateelektrode 11 ist mit einem Isolierfilm 10 bedeckt. Auf dem Isolierfilm 10 ist die Halbleiterschicht 1 gebildet. Als beispielhafte Materialien für diese Elemente ist der Isolierfilm 12 aus Siliziumoxid gebildet, die Gateelektrode 11 ist aus mit Dotierstoff dotiertem Polysilizium gebildet, der Isolierfilm 10 ist aus Siliziumoxid wie TEOS gebildet, und die Halbleiterschicht 1 ist aus Silizium gebildet.

[0207] In der Halbleiterschicht 1 sind ein Kanalbereich 2, der über der Gateelektrode 11 positioniert ist, ein Sourcebereich 3 und ein Drainbereich 4, die den Kanalbereich 2 einschließen, gebildet. Ein Abschnitt des Isolierfilmes 10 in Kontakt mit dem Kanalbereich 2 dient als ein Gateisolierfilm. Bei den Beispielen von Fig. 3 und 5 ist der Leitungstyp des Kanalbereiches 2 vom n-Typ, und der Leitungstyp des Sourcebereiches 3 und des Drainbereiches 4 ist vom p-Typ. Als Beispiel ist speziell der TFT 100 als ein p-Kanal-MOS-TFT gebildet. Unnötig zu sagen, daß der TFT 100 als ein n-Kanal-MOS-TFT gebildet sein kann.

[0208] Die Halbleiterschicht 1 ist als eine polykristalline Halbleiterschicht gebildet und enthält, wie in Fig. 3 gezeigt ist, eine Vielzahl von Körnern 5 und eine Korngrenze 6, die an einer Schnittstelle dazwischen gebildet ist und eine Kristallstörung aufweist. Eine Kristallorientierung ist in jedem Kristallkorn 5 gleichförmig, während die Kristallorientierungen im allgemeinen unter verschiedenen Kristallkörnern 5 unterschiedlich sind. Die Größe und Anordnung der Körner 5 ist zufällig und variiert bei dem Vorgang des Bildens der Halbleiterschicht 1. Genauer, selbst wenn eine Menge von TFTs 101 durch den gleichen Herstellungsvorgang hergestellt wird, variiert die Kristallstruktur der Halbleiterschicht 1 von einem TFT 101 zu einem anderen.

[0209] Als Resultat, es sei angenommen, daß der TFT 101 eine Einheit darstellt und ein TFT 102 sich von dem TFT 101 als eine Einheit unterschiedlich zu dem TFT 101 unterscheidet und durch den gleichen Herstellungsvorgang wie der des TFT 101 hergestellt ist, wie in Fig. 5 gezeigt ist, der Betrag der Korngrenzen 600, die den Kanalbereich 2 in dem TFT 101 belegt, ist nicht gleich der des TFT 102. Fig. 5 zeigt ein Beispiel des TFT 102, der weniger Korngrenzen 6 in dem Kanalbereich 2 als der TFT 1 aufweist.

[0210] Bezüglich des polykristallinen TFT ist es bekannt, daß eine Eigenschaft mit dem Betrag von Korngrenzen 6 variiert, die in dem Kanalbereich 2 enthalten sind. Dieses ist zum Beispiel in IEEE Transactions on Electronic Devices, Bd. 45, Nr. 1, Januar 1998, S. 165-172 gezeigt (Druckschrift 3). Insbesondere ist, wie Fig. 6 die Beziehung zwischen der Gatespannung V_g und dem Drainstrom I_d der TFTs 101 und 102 zeigt, der Drainstrom I_d in dem TFT 101, in dem mehr Korngrenzen 6 in dem Kanalbereich 2 enthalten sind, kleiner bei der gleichen Gatespannung V_{g0} als bei dem TFT 102, bei dem weniger Korngrenzen 6 in dem Kanalbereich 2 enthalten sind ($I_{da} > I_{db}$).

[0211] Daher kann die Variation der Kristallstruktur der polykristallinen Substanz des TFT 100 zur Identifikation des Halbleitersubstrates benutzt werden. Da die elektrische Eigenschaft, die sich von einem Halbleitersubstrat zu einem anderen unterscheidet, durch die Variation der Kristallstruktur der polykristallinen Substanz verursacht wird, kann die elektrische Eigenschaft nicht von außen neu geschrieben werden anders als der Identifikationscode, der in dem Flash-Speicher 908 aufgezeichnet ist (Fig. 65). Daher ist es möglich, das Sicherheitsniveau gegen die betrügerische Benutzung des Gerätes zu verbessern.

[0212] Weiterhin ist ungleich der Technik des Program-

mierens des Identifikationscodes in den Flash-Speicher 908 die Arbeit des Programmierens hier nicht notwendig. Da weiterhin die sich von einem Halbleitersubstrat zu dem anderen unterscheidende Eigenschaft durch den gleichen Herstellungsvorgang erzielt werden kann anders als die Technik des Aufzeichnens des Identifikationscodes in den Masken-ROM, wird der Herstellungsvorgang vereinfacht, und die Zahl der Prozeßschritte und die Herstellungskosten können verringert werden. Weiterhin ist die Variation in den Kristallstrukturen der polykristallinen Substanzen groß, und folglich ist die Variation der elektrischen Eigenschaften, die durch Variation der Kristallstrukturen verursacht wird, groß. Daher ist es möglich, einen großen Bereich der Variation bei den Identifikationscodes Cd sicherzustellen.

[0213] Mit anderen Worten, es ist leicht eine Übereinstimmung der Identifikationscodes unter einer Menge von massenproduzierten Halbleitervorrichtungen 600 zu verhindern.

[0214] Obwohl der Herstellungsvorgang kompliziert ist, kann es einen anderen Aufbau geben, bei dem nur der Kanalbereich 2 aus dem polykristallinen Halbleiter gebildet ist und der Sourcebereich 3 und der Drainbereich 4 aus Einkristallhalbleiter gebildet sind, auch in diesem Fall variiert die Eigenschaft zufällig.

[0215] Die elektrische Eigenschaft des in Fig. 2 bis 6 gezeigten Halbleiterelementes 401 kann sich ein wenig durch die Änderung der Temperatur und der Zeit ändern. Es wird folglich angenommen, daß der Identifikationscode Cd nicht vollständig einen konstanten Wert hält und in einem gewissen Grad variiert. Um dieses Problem zu lösen, muß die Komperatorschaltung 403 die Übereinstimmung der Identifikationscodes innerhalb eines Spielraumes in Hinblick auf die Änderung des Identifikationscodes Cd beurteilen.

[0216] Als ein Beispiel des Halbleiterelementes 401 mit der polykristallinen Substanz können neben den in Fig. 3 bis 6 gezeigten TFTs andere Elemente wie ein Widerstandselement mit der polykristallinen Substanz und ein kapazitives Element mit der polykristallinen Substanz benutzt werden. Weiterhin kann das Halbleiterelement 401 eine Mehrzahl von TFTs und ähnliches enthalten. Wenn die Zahl der TFTs zunimmt, wird die Variation der Identifikationscodes Cd größer. Dieses wird später im einzelnen bei der zwölften Ausführungsform erörtert.

1.3. OTPROM benutzendes Beispiel

[0217] Fig. 7 ist ein Blockschaltbild, das einen internen Aufbau der Codeerzeugereinheit 400 zeigt. Bei dem Beispiel von Fig. 7 weist die Codeerzeugereinheit 400 einen OTP-(einmal programmierbar)-ROM 602 auf, der ein nicht-flüchtiger Speicher ist, der nur einmal programmierbar ist. Vor der Versendung der Halbleitervorrichtung 600 wird der Identifikationscode Cd in den OTPROM 602 geschrieben. Nachdem die Halbleitervorrichtung 600 an den Benutzer geliefert ist, ist es danach technisch unmöglich, den in den OTPROM 602 geschriebenen Identifikationscode Cd neu zu schreiben. Mit andern Worten, bei dem Beispiel von Fig. 7 kann eine hohe technische Barriere gegen die betrügerische Benutzung des Identifikationscodes Cd, der von der Codeerzeugereinheit 400 erzeugt ist, vorteilhafterweise erzielt werden.

[0218] Der OTPROM ist geeignet zur Benutzung in dem Speicher 601, wie in Fig. 8 gezeigt ist, als auch in der Codeerzeugereinheit 400. Bei dem Beispiel von Fig. 8 weist der Speicher 601 den OTPROM 602 auf. Vor der Verwendung der Halbleitervorrichtung 600 wird der von der Codeerzeugereinheit 400 übertragene Identifikationscode Cd in den OTPROM 602 in dem Speicher 601 als der Speichercode Co geschrieben. Nachdem die Halbleitervorrichtung

600 an den Benutzer geliefert ist, ist es danach technisch unmöglich, den in den OTPROM 602 geschriebenen Speichercode Co neu zu schreiben. Mit andern Worten, bei dem Beispiel von Fig. 8 wird eine hohe technische Barriere gegen die betrügerische Benutzung des in dem Speicher 601 gespeicherten Speichercode Co vorteilhafterweise erzielt. Es ist auch möglich, eine betrügerische Benutzung durch Ersetzen des Halbleitersubstrates, in dem die Codeerzeugereinheit 400 gebildet ist und neu Schreiben des Speichercode Co, der in dem Speicher 601 gespeichert ist, zur gleichen Zeit, so daß er mit dem Identifikationscode Cd eines neuen Halbleitersubstrates übereinstimmt.

1.4. Anschlußeinrichtung

[0219] Fig. 9 ist ein Blockschaltbild, das einen Aufbau einer Anschlußeinrichtung als ein Gerät der Halbleitervorrichtung 600 zeigt. Die Anschlußeinrichtung 1001 ist als Mobiltelefon aufgebaut. Eine Halbleitervorrichtung 1002 in der Anschlußeinrichtung 1001 ist ein Beispiel der in Fig. 1 gezeigten Halbleitervorrichtung 600 und weist eine Kommunikationsschaltung 405a als die vorbestimmte Schaltung 405 auf. Obwohl es bevorzugt ist, daß die Codeerzeugereinheit 400, die Komperatorschaltung 403 und die Kommunikationsschaltung 405a in einem einzigen Halbleitersubstrat CH100 gebildet werden, können nur die Komperatorschaltung 403 und die Codeerzeugereinheit 400 in einem einzigen Halbleitersubstrat CH102 gebildet werden, oder nur die Codeerzeugereinheit 400 kann in einem einzigen Halbleitersubstrat gebildet werden. In jedem Fall ist ein Speicher 654, der den Speichercode Co speichert, in einem Halbleitersubstrat CH51 unterschiedlich von dem Halbleitersubstrat gebildet, in dem die Codeerzeugereinheit 400 gebildet ist.

[0220] Eine gemeinsame Kommunikationsträger-(als "Station" bezeichnet falls notwendig) Ausrüstung 655, die eine Ausrüstung des gemeinsamen Kommunikationsträgers ist, durch den die Kommunikation der Anschlußeinrichtung 1001 durchgeführt wird, weist eine Kommunikationsschaltung 656 auf. Zwischen der Kommunikationsschaltung 405a und der Kommunikationsschaltung 656 wird ein Kommunikationssignal dessen Inhalte Stimme, Daten und ähnliches sind, drahtlos übertragen (mit Funkwellen/Radiowellen). Die Anschlußeinrichtung 1001 und die gemeinsame Kommunikationsträgersausrüstung 655 stellen ein Kommunikationssystem 1000 dar.

[0221] Fig. 10 ist ein Blockschaltbild, das einen beispielhaften inneren Aufbau der Kommunikationsschaltung 405a zeigt. Bei der Kommunikationsschaltung 405a, die in der Anschlußeinrichtung 1001 enthalten ist, wobei Funkwellen benutzt werden, sind eine gutbekannte Radiofrequenzschaltung 462 und eine Zwischenfrequenzschaltung 463 zwischen eine Antenne und eine Signalverarbeitungsschaltung (Basisbandschaltung) 900 eingefügt. Die Signalverarbeitungsschaltung 900 weist eine Senderschaltung 460 und eine Empfängerschaltung 461 auf, und ein Kommunikationssignal Dt wird von der Empfängerschaltung 461 empfangen und durch die Senderschaltung 460 übertragen.

[0222] Bei dem Beispiel von Fig. 10 wird nur die Senderschaltung 460 durch das Freigabesignal EN ein- und ausgeschaltet. Genauer, wenn die Komperatorschaltung 403 eine Beurteilung der Nichtübereinstimmung durchführt, wird eine Übertragungsfunktion gestoppt. Es kann einen anderen Aufbau der Kommunikationsschaltung 405 geben, bei dem nur die Empfängerschaltung 461 oder sowohl die Senderschaltung 460 als auch die Empfängerschaltung 461 aus- und eingeschaltet werden auf der Grundlage des Freigabesignales En.

[0223] Fig. 11 ist ein Flußdiagramm einer Prozedur für die

Benutzung der Anschlußeinrichtung **1001** für Kommunikation. Zuerst wird die Halbleitervorrichtung **600** (genauer eine Halbleitervorrichtung **1001**) als ein Teil hergestellt (S201). Während oder vor dem letzten Schritt wird der Identifikationscode Cd in dem Speicher **601** als der Speichercode Co aufgezeichnet (S202). Danach wird die Halbleitervorrichtung **600** an einen Telefonhersteller geliefert, und die Anschlußvorrichtung **1001** wird durch den Telefonhersteller zusammengesetzt (S203). Die fertige Anschlußeinrichtung **1001** wird an den Benutzer geliefert (S204), und sie dient zur Kommunikation durch den Benutzer (S205). Die Schritte S206 bis S210 zeigen eine Prozedur der Kommunikation unter Benutzung der Anschlußeinrichtung **1001**, d. h. ein interner Fluß des Schrittes S205. Wenn die Kommunikation gestartet wird, liest die Anschlußeinrichtung **1001** den Speichercode Co aus dem Speicher **601** aus (S206). Darauf folgend vergleicht die Komperatorschaltung **403** den Identifikationscode Cd mit dem Speichercode Co und erzeugt das Freigabesignal En, daß das Resultat der Beurteilung darstellt, ob diese Codes miteinander übereinstimmen oder nicht (S207).

[0224] Wenn das Freigabesignal En die Übereinstimmung der Codes anzeigt (S208), behält die Kommunikationsschaltung **405a** die Kommunikationsfunktion zum Fortsetzen der Kommunikation (S209). Andererseits zeigt das Freigabesignal En die Nichtübereinstimmung der Codes an (S208), die Kommunikationsschaltung **405a** stoppt mindestens eine der Übertragungsfunktion und der Empfangsfunktion zum Unmöglichmachen der Kommunikation (S210). Wenn die Kommunikation beendet ist, ist die Prozedur beendet.

[0225] Da mindestens eine der Funktionen der Kommunikationsschaltung **405a** in der Anschlußeinrichtung **1001** gestoppt wird, wenn das Freigabesignal En die Nichtübereinstimmung anzeigt, ist es somit möglich, automatisch einen Betrug des Benutzers der Anschlußeinrichtung zur Kommunikation durch Ersetzen des Halbleitersubstrates automatisch zu unterdrücken durch die Wirkung der Anschlußeinrichtung **1001** selbst ohne eine Prozedur der gemeinsamen Kommunikationsträgersausrüstung **655**.

[0226] Obwohl das Mobiltelefon, das die Kommunikation drahtlos ausführt, als Beispiel der Anschlußeinrichtung in der obigen Erörterung gezeigt wurde, kann diese Ausführungsform auf ein Drahttelefon angewendet werden, daß durch ein Kommunikationskabel kommuniziert. Weiter kann diese Ausführungsform auch auf verschiedene Anschlußeinrichtungen angewendet werden, die nicht auf das Telefon begrenzt sind.

[0227] Fig. 12 stellt verschiedene Anschlußeinrichtungen, auf die diese Ausführungsform angewendet werden kann, und verschiedene Server, mit denen die Anschlußeinrichtungen kommunizieren, dar. Zum Beispiel kann die Anschlußeinrichtung ein Fahrzeuganschluß sein, der mit einem Autobahnsteuersystem kommuniziert, das automatisch die Zahlung der Autobahnmaut und ähnliches steuert, oder eine IC-Karte oder ein Personalcomputer, von denen jeder mit einem ATM-System in einer Bank zum Abheben oder Einzahl von Bargeld kommuniziert.

2. Zweite Ausführungsform

[0228] Obwohl das einzelne Halbleitersubstrat durch den innewohnenden Identifikationscode in der Halbleitervorrichtung und der Anschlußeinrichtung der ersten Ausführungsform identifiziert wird, werden bei der zweiten Ausführungsform eine Mehrzahl von Halbleitersubstraten identifiziert.

[0229] Fig. 13 ist ein Blockschaltbild, das einen Aufbau einer Halbleitervorrichtung gemäß der zweiten Ausführungsform der vorliegenden Erfindung zeigt. Bei der Halbleitervorrichtung **620** von Fig. 13 ist der Speicher **601** in einem Halbleitersubstrat CH4 zusammen mit der Codeerzeugereinheit **400**, der Komperatorschaltung **403** und der vorbestimmten Schaltung **405** gebildet, und die Codeerzeugereinheit **400** und die Komperatorschaltung **403** sind in einem Halbleitersubstrat CH5 zusammen mit dem Speicher **601** gebildet. Die in dem Halbleitersubstrat CH4 gebildete Codeerzeugereinheit **400** erzeugt einen Identifikationscode Cd1, der dem Halbleitersubstrat CH4 inhärent ist/ihm innewohnt, und die in dem Halbleitersubstrat CH5 gebildete Codeerzeugereinheit **400** erzeugt einen Identifikationscode Cd2, der dem Halbleitersubstrat CH5 innewohnt/inhärent ist.

[0230] Der in dem Halbleitersubstrat CH4 gebildete Speicher **601** speichert den von der Codeerzeugereinheit **400**, die in dem Halbleitersubstrat CH5 gebildet ist, übertragenen Identifikationscode Cd2 als einen Speichercode Co2, und der in dem Halbleitersubstrat CH5 gebildete Speicher **601** speichert den von der Codeerzeugereinheit **400**, die in dem Halbleitersubstrat CH4 gebildet ist, übertragenen Identifikationscode Cd1 als einen Speichercode Co1. Genauer, die Identifikationscodes Cd1 und Cd2, die den Halbleitersubstraten CH4 bzw. CH5 innewohnen, werden in den Speichern **601** gespeichert, die jeweils in den anderen Halbleitersubstraten gebildet sind.

[0231] Die in dem Halbleitersubstrat CH4 gebildete Komperatorschaltung **403** vergleicht den Identifikationscode Cd1 mit dem Speichercode Co1, und die in dem Halbleitersubstrat CH5 gebildete Komperatorschaltung **403** vergleicht den Identifikationscode Cd2 mit dem Speichercode Co2. Die in dem Halbleitersubstrat CH4 gebildete vorbestimmte Schaltung **405** enthält einen Schaltungsabschnitt, der selektiv in einen aktiven Zustand oder einen inaktiven Zustand auf der Grundlage eines Paares von Freigabesignalen En1 und En2 kommt, die von den zwei Komperatorschaltungen **403** ausgegeben werden. Die vorbestimmte Schaltung **405** ist eine Kommunikationsschaltung ähnlich zu der Kommunikationsschaltung **405a** von zum Beispiel Fig. 10 und weist einen Aufbau auf zum Stoppen des Betriebes der Senderschaltung **460** auf, wenn mindestens eines der Freigabesignale En1 und En2 eine Nichtübereinstimmung der Code anzeigt. Dieses erhöht weiter die Barriere gegen die betrügerische Benutzung durch die Ersetzung des Halbleitersubstrates.

[0232] Die Zahl der Halbleitersubstrate, denen die innewohnenden Identifikationscodes Cd zugeordnet werden, können drei oder mehr sein. Zum Beispiel kann es einen anderen Aufbau geben, bei dem die Codeerzeugereinheit **400** zum Erzeugen des innewohnenden Identifikationscodes Cd und der Speicher **601** in jeder von drei Halbleitersubstraten gebildet sind und der Speicher **601** den von der Codeerzeugereinheit **400**, die in dem Halbleitersubstrat gebildet ist, das nicht das Halbleitersubstrat ist, in dem der Speicher **601** selbst gebildet ist, übertragenen Identifikationscode Cd speichert. Alternativ kann mindestens ein Teil der drei Speicher **601** in einem Halbleitersubstrat gebildet sein, das nicht eines der drei Halbleitersubstrate ist, in denen die Codeerzeugereinheiten **400** gebildet sind.

[0233] Wenn die Zahl von Halbleitersubstraten, denen die Identifikationscodes Cd gegeben wird, d. h. Halbleitersubstrate mit den Codeerzeugereinheiten **400**, zunimmt, kann eine höhere Barriere gegeben die betrügerische Benutzung des Gerätes erzielt werden. Da weiter der Speicher **601** nur in dem Halbleitersubstrat gebildet ist, das die Codeerzeugereinheit **400** aufweist, ist es möglich, die Zahl der Halbleitersubstrate auf ein Minimum zu senken. Bei der Halbleitervorrichtung **620** von Fig. 13 kann eine höhere Barriere ge-

gen die betrügerische Benutzung vorteilhafterweise erzielt werden, während die Zahl der Halbleitersubstrate auf zwei gedrückt wird, was gleich der Zahl von Halbleitersubstraten in der Halbleitervorrichtung 600 von Fig. 1 ist.

[0234] Fig. 14 ist ein Blockschaltbild, das einen Aufbau der Anschlußeinrichtung als Gerät der Halbleitervorrichtung 620 zeigt. Die Anschlußeinrichtung 1011 arbeitet als Mobiltelefon und stellt ein Kommunikationssystem 1010 mit der allgemeinen Kommunikationsträgersausrüstung 655 dar. Eine Halbleitervorrichtung 1012, die in der Anschlußeinrichtung 1011 enthalten ist, ist ein Beispiel der in Fig. 13 gezeigten Halbleitervorrichtung 620 und weist die Kommunikationsschaltung 405a als die vorbestimmte Schaltung 405 auf. Die Kommunikationsschaltung 405a stoppt ihre Funktion, wenn mindestens eines der Freigabesignale En1 und En2 die Nichtübereinstimmung der Codes anzeigt.

[0235] Obwohl es bevorzugt ist, daß die Codeerzeugereinheit 400 für die Erzeugung des Identifikationscodes Cd1, die Komperatorschaltung 403 zum Durchführen eines Vergleiches des Identifikationscodes Cd1, der Speicher 601 zum Speichern des Speichercode Co2 und die Kommunikationsschaltung 405a in einem einzelnen Halbleitersubstrat CH103 gebildet sind, kann es andere Aufbauten geben, in denen nur die Komperatorschaltung 403, der Speicher 601 und die Codeerzeugereinheit 400 in einem einzelnen Halbleitersubstrat CH11 gebildet sind und wobei nur die Codeerzeugereinheit 400 in einem einzelnen Halbleitersubstrat CH104 gebildet ist. Weiter ist es bevorzugt, daß der Speicher 601 zum Speichern des Speichercode Co1 in einem einzelnen Halbleitersubstrat CH13 zusammen mit der Codeerzeugereinheit 400 zum Erzeugen des Identifikationscode Cd2 und der Komperatorschaltung 403 zum Ausführen eines Vergleiches des Identifikationscodes Cd2 gebildet ist.

[0236] Fig. 15 ist ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung 1011. Zuerst wird die Halbleitervorrichtung 620 (genauer die Halbleitervorrichtung 1012) als ein Teil hergestellt (S241). Während oder vor der letzten Stufe des Schrittes S241 werden die Identifikationscodes Cd1 und Cd2 der Halbleitersubstrate in die Speicher 601 der jeweils anderen Halbleitersubstrate als die Speichercode Co1 und Co2 eingeschrieben (S242). Danach wird die Halbleitervorrichtung 620 an einen Telefonhersteller geliefert, und die Anschlußeinrichtung 1011 wird durch den Telefonhersteller zusammengesetzt (S243). Die fertige Anschlußeinrichtung 1011 wird an einen Benutzer geliefert (S244) und dient zur Kommunikation durch den Benutzer (S245).

[0237] Die Schritte S246 bis S250 zeigen eine Prozedur der Kommunikation unter Benutzung der Anschlußeinrichtung 1011, d. h. einen internen Fluß des Schrittes S245. Wenn die Kommunikation gestartet wird, liest die Anschlußeinrichtung 1011 die Speichercode Co1 und Co2 aus den zwei Speichern 601 aus (S246). Darauf folgend vergleicht eine der Komperatorschaltungen 403 den Identifikationscode Cd1 und den Speichercode Co1 zum Ausgeben des Freigabesignales En1, das das Beurteilungsergebnis darstellt, ob diese Codes miteinander übereinstimmen oder nicht, und zu der gleichen Zeit vergleicht die andere Komperatorschaltung 403 den Identifikationscode Cd2 und den Speichercode Co2 zum Ausgeben des Freigabesignales En2, das das Beurteilungsergebnis darstellt, ob diese Codes miteinander übereinstimmen oder nicht (S247).

[0238] Wenn beide Freigabesignale En1 und En2 die Übereinstimmung der Codes anzeigen (S248), hält die Kommunikationsschaltung 405a die Kommunikationsfunktion zum Fortsetzen der Kommunikation aufrecht (S249). Wenn andererseits mindestens eines der Freigabesignale En1 und En2 Nichtübereinstimmung der Codes anzeigt

(S248), stoppt die Kommunikationsschaltung 405 mindestens eine der Übertragungsfunktion und der Empfangsfunktion zum Sperren der Kommunikation (S250). Wenn die Kommunikation beendet ist, geht die Prozedur zu Ende.

3. Dritte Ausführungsform

[0239] Bei der dritten Ausführungsform wird eine Erörterung durchgeführt über eine Anschlußeinrichtung, die einen Abschnitt benutzt, wobei die vorbestimmte Schaltung in der Halbleitervorrichtung der ersten oder der zweiten Ausführungsform entfernt ist.

[0240] Fig. 16 ist ein Blockschaltbild, das einen Aufbau einer Anschlußeinrichtung gemäß der dritten Ausführungsform der vorliegenden Erfindung zeigt. Die Anschlußeinrichtung 1001 unterscheidet sich von der Anschlußeinrichtung 1001 der ersten Ausführungsform, die in Fig. 9 gezeigt ist, dadurch, daß die Kommunikationsschaltung 405a nicht den aktiven Zustand oder den inaktiven Zustand auswählt auf der Grundlage des Freigabesignales En, daß von der Komperatorschaltung 403 übertragen wird, sondern einfach das Freigabesignal En an die gemeinsame Kommunikationsschaltung 655 als Teil des Kommunikationssignales überträgt.

[0241] Der Fluß der Prozedur für die Benutzung der Anschlußeinrichtung 1001 von Fig. 16 für die Kommunikation ist ähnlich zu dem in Fig. 11 gezeigten. Der interne Fluß des Schrittes S205 wird jedoch durch die in Fig. 17 gezeigte Prozedur des Schrittes S1000 ersetzt. Wenn der Schritt S1000 startet, liest die Anschlußeinrichtung 1001 den Speichercode Co aus dem Speicher 601 aus (S206). Darauf folgend vergleicht die Komperatorschaltung 403 den Identifikationscode Cd und den Speichercode Co und erzeugt das Freigabesignal En, daß das Resultat der Beurteilung darstellt, ob diese Codes miteinander übereinstimmen oder nicht (S207).

[0242] Das Freigabesignal En wird zu der gemeinsamen Kommunikationsträgersausrüstung 655 durch die Kommunikationsschaltung 405a übertragen (S208, S1001, S1003). Mit andern Worten, wenn das Freigabesignal En die Übereinstimmung der Codes anzeigt (S208), wird ein vorbestimmter Wert, der die Übereinstimmung der Codes anzeigt, als das Freigabesignal En übertragen (S1001) und wenn das Freigabesignal En Nichtübereinstimmung der Codes anzeigt (S208), wird der vorbestimmte Wert nicht übertragen (S1003).

[0243] Die gemeinsame Kommunikationsträgersausrüstung 655 führt eine Authentifizierung durch, daß der Benutzer der Anschlußeinrichtung 1001 autorisiert ist, wenn das Freigabesignal En die Übereinstimmung der Codes anzeigt, und sie führt die Authentifizierung nicht durch, wenn das Freigabesignal En Nichtübereinstimmung der Codes anzeigt. Die gemeinsame Kommunikationsträgersausrüstung 655 ermöglicht, daß die Kommunikation den Kommunikationsprozeß fortsetzt (S1002), wenn die Authentifizierung durchgeführt ist, und sie erlaubt die Kommunikation nicht, so daß der Kommunikationsprozeß stoppt (S1004), wenn die Authentifizierung nicht durchgeführt ist.

[0244] Somit kann in der Anschlußeinrichtung 1001 von Fig. 16 das Freigabesignal En zur Beurteilung bei der Authentifikation dienen, die durch die gemeinsame Kommunikationsträgersausrüstung 655 durchgeführt wird, und die betrügerische Benutzung durch Ersetzen des Halbleitersubstrates wird dadurch ausgeschlossen bei der Authentifikation zum Erzielen einer Authentifikation mit hoher Genauigkeit. Weiter können nach dem Fortsetzen oder Stoppen der Kommunikation Vorsehen oder Nichtvorsehen von Dienstleistungen wie das Ermöglichen oder Nichtermöglichen ei-

ner Geschäftstätigkeit der Authentifikation folgen. Alternativ kann es einen anderen Fall geben, indem nur das Aufzeichnen der Beurteilungssache für die Authentifikation durchgeführt wird. Spezielle Beispiele werden in späteren Ausführungsformen erörtert.

[0245] Fig. 18 ist ein Blockschaltbild, das einen anderen Aufbau der Anschlußeinrichtung gemäß der dritten Ausführungsform der vorliegenden Erfindung zeigt. Die Anschlußeinrichtung 1011 unterscheidet sich von der in Fig. 14 gezeigten Anschlußeinrichtung 1011 der zweiten Ausführungsform dadurch, daß die Kommunikationsschaltung 405 nicht den aktiven Zustand oder den inaktiven Zustand auf der Grundlage der Freigabesignale En1 und En2 auswählt, die von den Komperatorschaltungen 403 übertragen werden, sondern einfach die Freigabesignale En1 und En2 an die gemeinsame Kommunikationsträgersausrüstung 655 als Teil des Kommunikationssignales überträgt.

[0246] Der Fluß der Prozedur für die Benutzung der Anschlußeinrichtung 1011 von Fig. 18 für die Kommunikation ist ähnlich zu dem in Fig. 15 gezeigten. Der interne Fluß des Schrittes S245 ist jedoch durch die Prozedur des in Fig. 19 gezeigten Schrittes 81010 ersetzt. Wenn der Schritt S1010 startet, liest die Anschlußeinrichtung 1011 die Speichercode Co1 und Co2 aus den zwei Speichern 601 aus (S246). Darauf folgend vergleicht eine der Komperatorschaltungen 403 den Identifikationscode Cd1 und den Speichercode Co1 zum Ausgeben des Freigabesignales En1, das das Beurteilungsergebnis darstellt, ob diese Codes miteinander übereinstimmen oder nicht, und zu der gleichen Zeit vergleicht die andere der Komperatorschaltungen 403 den Identifikationscode Cd2 und den Speichercode Co2 zum Ausgeben des Freigabesignales En2, das das Beurteilungsergebnis darstellt, ob diese Codes miteinander übereinstimmen oder nicht (S247).

[0247] Die Freigabesignale En1 und En2 werden an die gemeinsame Kommunikationsträgersausrüstung 655 durch die Kommunikationsschaltung 405a übertragen (S248, S1001, S1003). Mit anderen Worten, wenn beide Freigabesignale En1 und En2 Übereinstimmung der Codes anzeigen (S248), werden vorbestimmte Werte, die die Übereinstimmung der Codes bezeichnen, als die Freigabesignale En1 und En2 übertragen (S1001), und wenn mindestens eines der Freigabesignale En1 und En2 Nichtübereinstimmung der Codes bezeichnet (S248), werden die vorbestimmten Werte nicht übertragen (S1003).

[0248] Die gemeinsame Kommunikationsträgersausrüstung 655 führt eine Authentifikation durch, daß der Benutzer der Anschlußeinrichtung 1001 autorisiert ist, wenn beide Freigabesignale En1 und En2 Übereinstimmung der Codes anzeigen, und sie führt nicht die Authentifikation durch, wenn mindestens eines der Freigabesignale En1 und En2 eine Nichtübereinstimmung der Codes bezeichnet. Die gemeinsame Kommunikationsträgersausrüstung 655 ermöglicht der Kommunikation, daß sie den Kommunikationsprozeß fortsetzt (S1002), wenn die Authentifikation durchgeführt ist, und sie erlaubt die Kommunikation nicht zum Stoppen des Kommunikationsprozesses (S1004), wenn die Authentifikation nicht durchgeführt worden ist.

[0249] Somit können bei der Anschlußeinrichtung 1011 von Fig. 18 die Freigabesignale En1 und En2 zur Beurteilung bei der Authentifikation dienen, die durch die gemeinsame Kommunikationsträgersausrüstung 655 durchgeführt wird, und die betrügerische Benutzung durch Ersetzen des Halbleitersubstrates wird hierdurch bei der Authentifikation unterdrückt zum Erzielen einer Authentifikation mit hoher Genauigkeit. Da weiter zwei Freigabesignale En1 und En1 als Beurteilungssachen bei der Authentifikation benutzt werden, kann die Authentifikation mit noch höherer Genau-

igkeit als bei der Anschlußeinrichtung 1001 von Fig. 16 erzielt werden.

4. Vierte Ausführungsform

[0250] Bei der vierten Ausführungsform wird die Erörterung über eine Anschlußeinrichtung gegeben, die einen Abschnitt benutzt, wobei die vorbestimmte Schaltung und die Komperatorschaltung in der Halbleitervorrichtung der ersten oder der zweiten Ausführungsform entfernt sind.

[0251] Fig. 20 ist ein Blockschaltbild das einen Aufbau einer Anschlußeinrichtung gemäß der vierten Ausführungsform der vorliegenden Erfindung zeigt. Die Halbleitervorrichtung 652 in der Anschlußeinrichtung 801 unterscheidet sich von der Anschlußeinrichtung 1002 der ersten in Fig. 9 gezeigten Ausführungsform dadurch, daß die Komperatorschaltung 403 entfernt ist und die Kommunikationsschaltung 405a nur den Identifikationscode Cd und den Speichercode Co zu der gemeinsamen Kommunikationsträgersausrüstung 655 als Teil des Kommunikationssignales überträgt.

[0252] Die gemeinsame Kommunikationsträgersausrüstung 655 von Fig. 20 weist eine Beurteilungsschaltung 657 und einen Kundendatenbankspeicher 658 neben der Kommunikationsschaltung 656 auf. Die gemeinsame Kommunikationsträgersausrüstung 655 und die Anschlußeinrichtung 801 stellen das Kommunikationssystem 800 dar.

[0253] Der Fluß der Prozedur für die Benutzung der Anschlußeinrichtung 801 zur Kommunikation ist ähnlich zu dem in Fig. 11 gezeigten. Der interne Fluß des Schrittes S205 ist jedoch durch die in Fig. 21 gezeigte Prozedur des Schrittes S260 ersetzt. Wenn der Schritt S260 startet, überträgt die Anschlußeinrichtung 801 den Identifikationscode Cd und den Speichercode Co zu der gemeinsamen Kommunikationsträgersausrüstung 655 (S261). Folglich empfängt die Kommunikationsschaltung 656 in der gemeinsamen Kommunikationsträgersausrüstung 655 den Identifikationscode Cd und den Speichercode Co (S262).

[0254] Darauf folgend vergleicht die Beurteilungsschaltung 657 in der gemeinsamen Kommunikationsträgersausrüstung 655 den Identifikationscode Cd mit dem Speichercode Co und beurteilt, ob diese Codes miteinander übereinstimmen oder nicht zum Übertragen des Freigabesignales En, das das Beurteilungsergebnis anzeigt, zu der Kommunikationsschaltung 656 (S263). Wenn das Freigabesignal En Übereinstimmung anzeigt (S264), führt die gemeinsame Kommunikationsträgersausrüstung 655 eine Authentifikation durch, daß der Benutzer der Anschlußeinrichtung 801 autorisiert ist, und wenn das Freigabesignal En eine Nichtübereinstimmung anzeigt (S264), führt die gemeinsame Kommunikationsträgersausrüstung 655 keine Authentifikation durch. Die gemeinsame Kommunikationsträgersausrüstung 655 ermöglicht der Kommunikation, den Kommunikationsprozeß fortzusetzen (S265), wenn die Authentifikation durchgeführt ist, und sie erlaubt die Kommunikation nicht zum Stoppen des Kommunikationsprozesses (S268), wenn die Authentifikation nicht durchgeführt ist.

[0255] Wenn weiter angewiesen wird, den Identifikationscode Cd und den Speichercode Co aufzuzeichnen (S266), werden der Identifikationscode Cd und der Speichercode Co in den Kundendatenbankspeicher 658 eingeschrieben, wenn die Authentifikation nicht durchgeführt wird (S267). Dann wird, nachdem der Kommunikationsvorgang gestoppt ist (S268) durch Überprüfen des Identifikationscodes Cd und des Speichercode Co mit dem Inhalt des Kundendatenbankspeichers 258, der in der Vergangenheit aufgezeichnet ist (S269), ein unautorisierte Benutzer spezifiziert (S270).

[0256] Es kann einen anderen Fall geben, in dem nur das Aufzeichnen des Identifikationscodes Cd und des Speicher-

codes Co durchgeführt wird (S267), ohne daß der Kommunikationsprozeß gestoppt wird, wenn die Authentifikation nicht durchgeführt wird. Es kann einen noch anderen Fall geben, in dem das Aufzeichnen des Identifikationscodes Cd und des Speichercode Co durchgeführt wird (S267) unabhängig von dem Authentifikationsresultat. In dem letzteren Fall wird die Prozedur des Schrittes S267 zwischen den Schritten S263 und S264 zum Beispiel durchgeführt.

[0257] Somit können bei der Anschlußeinrichtung 801 von Fig. 20 der Identifikationscode Cd und der Speichercode Co zur Beurteilung bei der Authentifikation dienen, die von der gemeinsamen Kommunikationsträgerausrüstung 655 durchgeführt wird, und die betrügerische Benutzung durch Ersetzen des Halbleitersubstrates wird dadurch in der Authentifikation unterdrückt zum Erzielen der Authentifikation mit hoher Genauigkeit.

[0258] Fig. 22 ist ein Blockschaltbild, das einen anderen Aufbau der Anschlußeinrichtung gemäß der vierten Ausführungsform der vorliegenden Erfindung zeigt. Die Halbleitervorrichtung 652 in der Anschlußeinrichtung 811 unterscheidet sich von der Anschlußeinrichtung 1012 in der in Fig. 14 gezeigten zweiten Ausführungsform dadurch, daß die Komparatorschaltung 403 entfernt ist und die Kommunikationsschaltung 405 nur die Identifikationscodes Cd1 und Cd2 und die Speichercode Co1 und Co2 an die gemeinsame Kommunikationsträgerausrüstung 655 als Teil des Kommunikationssignales überträgt.

[0259] Die gemeinsame Kommunikationsträgerausrüstung 655 von Fig. 22 weist die Beurteilungsschaltung 657 und den Kundendatenbankspeicher 658 neben der Kommunikationsschaltung 656 auf. Die gemeinsame Kommunikationsträgerausrüstung 655 und die Anschlußeinrichtung 811 stellen das Kommunikationssystem 810 dar.

[0260] Der Fluß der Prozedur für die Benutzung der Anschlußeinrichtung 811 für die Kommunikation ist ähnlich zu dem in Fig. 15 gezeigten. Der interne Fluß des Schrittes S245 ist jedoch durch die in Fig. 23 gezeigte Prozedur des Schrittes S280 ersetzt. Wenn der Schritt S280 startet, überträgt die Anschlußeinrichtung 811 die Identifikationscodes Cd1 und Cd2 und die Speichercode Co1 und Co2 zu der gemeinsamen Kommunikationsträgerausrüstung 655 (S271). Folglich empfängt die Kommunikationsschaltung 656 in der gemeinsamen Kommunikationsträgerausrüstung 655 die Identifikationscodes Cd1 und Cd2 und die Speichercode Co1 und Co2 (S272).

[0261] Darauf folgend vergleicht die Beurteilungsschaltung 657 in der gemeinsamen Kommunikationsträgerausrüstung 655 den Identifikationscode Cd1 mit dem Speichercode Co1 zum Beurteilen, ob diese Codes miteinander übereinstimmen oder nicht, und sie vergleicht den Identifikationscode Cd2 mit dem Speichercode Co2 zum Beurteilen, ob diese Codes miteinander übereinstimmen oder nicht. Die Beurteilungsschaltung 657 überträgt das Freigabesignal En, daß diese Beurteilungsergebnisse anzeigen, zu der Kommunikationsschaltung 656 (S273). Wenn beide Vergleichsergebnisse Übereinstimmung anzeigen (S274), führt die gemeinsame Kommunikationsträgerausrüstung 655 eine Authentifikation durch, daß der Benutzer der Anschlußeinrichtung 811 autorisiert ist, und wenn mindestens eines der zwei Vergleichsergebnisse eine Nichtübereinstimmung anzeigt (S274), führt die gemeinsame Kommunikationsträgerausrüstung 655 nicht die Authentifikation durch. Die gemeinsame Kommunikationsträgerausrüstung 655 erlaubt der Kommunikation, den Kommunikationsvorgang fortzusetzen (S275), wenn die Authentifikation durchgeführt ist, und sie erlaubt nicht die Kommunikation zum Stoppen des Kommunikationsvorganges (S278), wenn die Authentifikation nicht durchgeführt ist.

[0262] Wenn weiter angeordnet ist, die Identifikationscodes Cd1 und Cd2 und die Speichercode Co1 und Co2 aufzuzeichnen (S276), werden die Identifikationscodes Cd1 und Cd2 und die Speichercode Co1 und Co2 in dem Kundendatenbankspeicher 658 aufgezeichnet, wenn die Authentifikation nicht durchgeführt wird (S277). Dann wird zum Beispiel, nachdem der Kommunikationsvorgang gestoppt ist (S278), durch Prüfen der Identifikationscodes Cd1 und Cd2 und der Speichercode Co1 und Co2 mit dem Inhalt des Kundendatenbankspeichers 658, der in der Vergangenheit aufgezeichnet ist (S279), ein unautorisierter Benutzer spezifiziert (S280).

[0263] Es kann einen anderen Fall geben, indem nur das Aufzeichnen der Identifikationscodes Cd1 und Cd2 und der Speichercode Co1 und Co2 durchgeführt wird (S277) ohne Stoppen des Kommunikationsvorganges, wenn die Authentifikation nicht durchgeführt wird. Weiter kann es noch einen Fall geben, in dem das Aufzeichnen der Identifikationscodes Cd1 und Cd2 und der Speichercode Co1 und Co2 durchgeführt wird (S277) unabhängig von dem Authentifikationsresultat. In dem letzteren Fall wird die Prozedur des Schrittes S277 zwischen den Schritten S273 und S274 zum Beispiel durchgeführt.

[0264] Somit können bei der Anschlußeinrichtung 811 von Fig. 22 die Identifikationscodes Cd1 und Cd2 und die Speichercode Co1 und Co2 zur Beurteilung bei der Authentifikation dienen, die durch die gemeinsame Kommunikationsträgerausrüstung 655 durchgeführt wird, und die betrügerische Benutzung durch Ersetzen des Halbleitersubstrates wird dadurch bei der Authentifikation unterdrückt zum Erzielen der Authentifikation mit hoher Genauigkeit. Da weiter die zwei Identifikationscodes Cd1 und Cd2 in dem Vergleich benutzt werden, kann die Authentifikation mit noch höherer Genauigkeit als in der Anschlußeinrichtung 801 von Fig. 20 erzielt werden.

5. Fünfte Ausführungsform

[0265] Bei der fünften Ausführungsform werden der Identifikationscode Cd und der Speichercode Co in verschlüsselter Form zwischen den Halbleitersubstraten bei der Halbleitervorrichtung der ersten oder zweiten Ausführungsform übertragen.

[0266] Fig. 24 ist ein Blockschaltbild, das einen Aufbau einer Halbleitervorrichtung gemäß der fünften Ausführungsform der vorliegenden Erfindung zeigt. Bei der Halbleitervorrichtung 630 von Fig. 24 sind eine Verschlüsselungsschaltung 631, eine Decodierschaltung 632 und eine Schlüsselerzeugereinheit 633 in einem Halbleitersubstrat CH20 oder CH22 gebildet, in dem die Codeerzeugereinheit 400 gebildet ist.

[0267] Die Schlüsselerzeugereinheit 633 erzeugt einen Schlüssel K für die Verschlüsselung. Der Schlüssel K wird als Code erzeugt, der dem Halbleitersubstrat CH20 oder CH22 innewohnt oder inhärent ist, wie der Identifikationscode Cd. Die Verschlüsselungsschaltung 631 verschlüsselt den Identifikationscode Cd, der von der Codeerzeugereinheit 400 erzeugt ist, auf der Grundlage des Schlüssels K, der von der Schlüsselerzeugereinheit 633 erzeugt ist, in einen Identifikationscode Cd# und überträgt den Identifikationscode Cd# an den Speicher 601, der in einem Halbleitersubstrat CH21 gebildet ist. Der Speicher 601 speichert den verschlüsselten Identifikationscode Cd# als verschlüsselten Speichercode Co#.

[0268] Die Decodierschaltung 632 liest den in dem Speicher 601 gespeicherten Speichercode Co#, decodiert den Speichercode Co# in den Speichercode Co auf der Basis des Schlüssels K, der von der Schlüsselerzeugereinheit 633 er-

zeugt ist, und liefert den Speichercode Co an die Komperatorschaltung 403. Die vorbestimmte Schaltung 405 enthält einen Schaltungsabschnitt, der selektiv in einen aktiven Zustand oder einen inaktiven Zustand kommt auf der Grundlage des Freigabesignales En, das von der Komperatorschaltung 403 ausgegeben wird.

[0269] Da der Identifikationscode Cd und der Speichercode Co in der verschlüsselten Form zwischen den verschiedenen Halbleitersubstraten in der Halbleitereinrichtung 630 übertragen werden, kann weder der Identifikationscodes Cd noch der Speichercode Co von der Außenseite gelesen werden. Daher kann eine höhere Barriere gegen die betrügerische Benutzung erzielt werden.

[0270] Fig. 25 ist ein Blockschaltbild das einen beispielhaften internen Aufbau der Schlüsselerzeugereinheit 633 zeigt. Bei dem Beispiel von Fig. 25 weist die Schlüsselerzeugereinheit 633 den OTPROM 602 auf, und vor dem Versenden der Halbleitervorrichtung 630 wird der Schlüssel K in den OTPROM 602 geschrieben. Daher ist es unmöglich, betrügerisch den Schlüssel K zu ändern, der von der Schlüsselerzeugereinheit 633 erzeugt ist. Da weiter der Schlüssel K bei der Versendung der Halbleitervorrichtung 630 geschrieben worden ist, wird der Schlüssel K daran gehindert, zu dem Benutzer herauszulecken.

[0271] Fig. 26 ist ein Blockschaltbild, das einen anderen internen Aufbau der Schlüsselerzeugereinheit 633 zeigt. Die Schlüsselerzeugereinheit 633 von Fig. 16 weist das Halbleiterelement 401 und die Codierschaltung 402 auf, die in Fig. 2 gezeigt sind. Die Codierschaltung 402 liest die elektrische Eigenschaft des Halbleiterelementes 401 als Analogsignal an und wandelt es in das Digitalsignal um. Das durch die Umwandlung erhaltene digitale Signal wird als der Schlüssel K ausgegeben.

[0272] Als elektrische Eigenschaft des Halbleiterelementes 401 wird eine Eigenschaft gewählt, die von einem Halbleiterelement 401 zu einem anderen variiert. Der Schlüssel K, der als ein Wert erzeugt wird, der von einem Halbleiterelement 401 zu einem anderen variiert, ist dem Halbleitersubstrat innewohnend/inhärent, in der die Schlüsselerzeugereinheit 633 gebildet ist. Da es nicht notwendig ist, den Schlüssel K zu schreiben, und die Halbleiterelemente 401, die durch den gleichen Herstellungsvorgang hergestellt werden, unter einer Menge von massenproduzierten Halbleitervorrichtungen 630 benutzt werden können, kann der Herstellungsvorgang der Halbleitervorrichtung 630 vereinfacht werden. Da weiter die elektrische Eigenschaft des Halbleiterelementes 401, auf der der Schlüssel K beruht, nicht von außen geändert werden kann, ist die Barriere gegen die betrügerische Änderung des Schlüssels K vorteilhafterweise hoch.

[0273] Wie in Fig. 3 bis 6 dargestellt ist, weist das Halbleiterelement 401 eine polykristalline Substanz auf, und die elektrische Eigenschaft, die mit der Variation in den Kristallstrukturen der polykristallinen Substanzen variiert, kann benutzt werden. Da die Variationen der Kristallstrukturen der polykristallinen Substanzen groß ist und folglich die Variation in den elektrischen Eigenschaften, die durch die Variation in den Kristallstrukturen verursacht wird, entsprechend groß ist, ist es möglich, einen großen Bereich von Variation in den Schlüsseln K sicherzustellen. Mit andern Worten, es ist leicht eine Übereinstimmung der Schlüssel K aus einer Menge von massenproduzierten Halbleitervorrichtung 630 zu verhindern.

[0274] Fig. 27 ist ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung 1001 von Fig. 9 für die Kommunikation, wenn die Halbleitervorrichtung 630 von Fig. 24 anstelle der Halbleitervorrichtung 1002 benutzt wird und wenn die Kommunikationsschaltung 405a als die

vorbestimmte Schaltung 405 in der Anschlußeinrichtung 1001 benutzt wird. Zuerst wird die Halbleitervorrichtung 630 als ein Teil hergestellt (S301). Während oder vor dem letzten Schritt wird der verschlüsselte Identifikationscode Cd# in den Speicher 601 als der Speichercode Co# geschrieben (S302). Danach wird die Halbleitervorrichtung 630 einem Telefonhersteller geliefert, und die Anschlußeinrichtung 1001 wird durch den Telefonhersteller zusammengebaut (S303). Die fertige Anschlußeinrichtung 1001 wird einem Benutzer geliefert (S304) und dient zur Kommunikation durch den Benutzer (S305).

[0275] Die Schritte S306 bis S310 zeigen eine Prozedur der Kommunikation unter Benutzung der Anschlußeinrichtung 1001, d. h. einen internen Fluß des Schrittes S305. Wenn die Kommunikation gestartet wird, liest die Anschlußeinrichtung 1001 den Speichercode Co# aus dem Speicher 601 aus (S306). Darauf folgend decodiert die Decodierschaltung 632 den Speichercode Co# in den Speichercode Co, und danach vergleicht die Komperatorschaltung 403 den Identifikationscode Cd und den Speichercode Co und erzeugt das Freigabesignal En, daß das Resultat der Beurteilung darstellt, ob diese Codes miteinander übereinstimmen oder nicht (S307).

[0276] Wenn das Freigabesignal En die Übereinstimmung der Codes anzeigt (S308), hält die Kommunikationsschaltung 405a die Kommunikationsfunktion zum Fortsetzen der Kommunikation (S309) aufrecht. Wenn andererseits das Freigabesignal En Nichtübereinstimmung der Codes anzeigt (S308), stoppt die Kommunikationsschaltung 405 mindestens eine der Übertragungsfunktion und der Empfangsfunktion zum Sperren der Kommunikation (S310). Wenn die Kommunikation beendet ist, ist die Prozedur zu Ende.

[0277] Fig. 28 ist ein Blockschaltbild, das einen anderen Aufbau der Halbleitervorrichtung gemäß der fünften Ausführungsform der vorliegenden Erfindung zeigt. Die Halbleitervorrichtung 635 von Fig. 28 weist einen Aufbau auf, bei dem die Identifikationscodes Cd1 und Cd2 und die Speichercode Co1 und Co1 in einer verschlüsselten Form zwischen den zwei Halbleitersubstraten in der Halbleitervorrichtung 620 von Fig. 13 übertragen werden. Genauer, die Verschlüsselungsschaltung 631, die Decodierschaltung 632 und die Schlüsselerzeugereinheit 633 sind in den beiden Halbleitersubstraten CH20 (oder CH22) und CH23 gebildet, in denen die Codeerzeugereinheit 400, die Komperatorschaltung 403 und der Speicher 601 gebildet sind.

[0278] In dem Halbleitersubstrat CH20 (oder CH22) erzeugt die Schlüsselerzeugereinheit 633 einen Schlüssel K1, der dem Halbleitersubstrat CH20 (oder CH22) innewohnt, und die Verschlüsselungsschaltung 631 verschlüsselt den Identifikationscode Cd1 in einen Identifikationscode Cd1# auf der Grundlage des Schlüssels K1 und überträgt den Identifikationscode Cd1# an den Speicher 601 in dem Halbleitersubstrat CH23. Der Speicher 601 in dem Halbleitersubstrat CH23 speichert den Identifikationscode Cd1# als einen Speichercode Co1#. Die Decodierschaltung 632 in dem Halbleitersubstrat CH20 (oder CH22) liest den Speichercode Co1# aus dem Speicher 601 aus, decodiert den Speichercode Co1# in den Speichercode Co1 auf der Grundlage des Schlüssels K1 und liefert den Speichercode Co1 an die Komperatorschaltung 403.

[0279] In dem Halbleitersubstrat CH23 erzeugt die Schlüsselerzeugereinheit 633 einen Schlüssel K2, der dem Halbleitersubstrat CH23 innewohnt, und die Verschlüsselungsschaltung 631 verschlüsselt den Identifikationscode Cd2 in einen Identifikationscode Cd2# auf der Grundlage des Schlüssels K2 und überträgt den Identifikationscode Cd2# an den Speicher 601 in dem Halbleitersubstrat CH20 (oder CH22). Der Speicher 601 in dem Halbleitersubstrat

CH20 (oder CH22) speichert den Identifikationscode Cd2# als einen Speichercode Co2#. Die Decodierschaltung 632 in dem Halbleitersubstrat CH23 liest den Speichercode Co2# aus dem Speicher 601 aus, decodiert den Speichercode Co2# in den Speichercode Cd2 auf der Grundlage des Schlüssels K2 und liefert den Speichercode Co1 an die Komperatorschaltung 403. Die vorbestimmte Schaltung 405 enthält einen Schaltungsabschnitt, der selektiv in einen aktiven Zustand oder einen inaktiven Zustand kommt auf der Grundlage eines Paares von Freigabesignalen En1 und En2, die von den zwei Komperatorschaltungen 403 ausgegeben sind.

[0280] Da somit die Identifikationscodes Cd1 und Cd2 und die Speichercodes Co1 und Co2 in der verschlüsselten Form zwischen den verschiedenen Halbleitersubstraten in der Halbleitervorrichtung 635 übertragen werden, kann keiner der Identifikationscodes Cd1 und Cd2 und der Speichercode Co1 und Co2 von der Außenseite gelesen werden. Daher kann eine höhere Barriere gegen die betrügerische Benutzung erzielt werden. Da die zwei Freigabesignale En1 und En2 benutzt werden wie in der Halbleitervorrichtung 620 der zweiten bevorzugten Ausführungsform (Fig. 13), ist es möglich, eine höhere Barriere gegen die betrügerische Benutzung durch die Ersetzung des Halbleitersubstrates zu erzielen.

[0281] Auch wenn die Zahl von Halbleitersubstraten, in denen die Codeerzeugereinheiten 400 gebildet sind, drei oder mehr beträgt, ist es durch Bilden der Verschlüsselungsschaltung 631, der Decodierschaltung 632 und der Schlüsselerzeugereinheit 633 in jedem der Halbleitersubstrate möglich, die Identifikationscodes und die Speichercodes in der verschlüsselten Form zwischen den verschiedenen Halbleitersubstraten zu übertragen.

[0282] Fig. 29 ist ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung 1011 zur Kommunikation, wenn die Halbleitervorrichtung 635 von Fig. 28 benutzt wird anstelle der Halbleitervorrichtung 1012, und die Kommunikationsschaltung 405a wird als die vorbestimmte Schaltung 405 in der Anschlußeinrichtung 1011 benutzt. Zuerst wird die Halbleitervorrichtung 635 als ein Teil hergestellt (S341). Während oder vor dem letzten Schritt werden die verschlüsselten Identifikationscodes Cd1# und Cd2# in dem Speicher 601 des anderen Halbleitersubstrates als die Speichercodes Co#1 und Co#2 eingeschrieben (S342). Danach wird die Halbleitervorrichtung 635 einem Telefonhersteller geliefert, und die Anschlußeinrichtung 1011 wird durch den Telefonhersteller zusammengebaut (S343). Die fertige Anschlußeinrichtung 1011 wird einem Benutzer geliefert (S344) und dient zur Kommunikation durch den Benutzer (S345).

[0283] Die Schritte S346 bis S350 zeigen eine Prozedur der Kommunikation unter Benutzung der Anschlußeinrichtung 1011, d. h. einen internen Fluß des Schrittes S345. Wenn die Kommunikation startet, liest die Anschlußeinrichtung 1011 die Speichercodes Co1# und Co2# aus den zwei Speichern 601 aus (S346). Darauf folgend decodiert die Decodierschaltung 632 die Speichercodes Co1# und Co2# in die Speichercodes Co1 und Co2, und danach vergleicht eine der Komperatorschaltungen 403 den Identifikationscode Cd1 und den Speichercode Co1 zum Ausgeben eines Freigabesignales En1, das das Beurteilungsergebnis darstellt, ob diese Codes miteinander übereinstimmen oder nicht, und zu der gleichen Zeit vergleicht die andere der Komperatorschaltungen 403 den Identifikationscode Cd2 und den Speichercode Co2 zum Ausgeben des Freigabesignales En2, das das Beurteilungsergebnis darstellt, ob diese Codes miteinander übereinstimmen oder nicht (S347).

[0284] Wenn die beiden Freigabesignale En1 und En2

Übereinstimmung der Codes anzeigen (S348), hält die Kommunikationsschaltung 405a die Kommunikationsfunktion zum Fortsetzen der Kommunikation (S349) aufrecht. Wenn andererseits mindestens eines der Freigabesignale En1 und En2 Nichtübereinstimmung dieser Codes anzeigt (S348), stoppt die Kommunikationsschaltung 405a mindestens eine der Übertragungsfunktion und der Empfangsfunktion zum Sperren der Kommunikation (S350). Wenn die Kommunikation beendet ist, endet die Prozedur.

6. Sechste Ausführungsform

[0285] Bei der sechsten Ausführungsform wird eine Diskussion über einen Aufbau gegeben, bei dem eine Umschalterschaltung zum exklusiven Ausführen einer Übertragung des verschlüsselten Informationscodes und Eingabe des verschlüsselten Speichercodes in der Halbleitervorrichtung der fünften Ausführungsform vorgesehen ist.

[0286] Fig. 30 ist ein Blockschaltbild, das einen Aufbau einer Halbleitervorrichtung gemäß der sechsten Ausführungsform der vorliegenden Erfindung zeigt. Bei der Halbleitervorrichtung 640 von Fig. 30 ist eine Umschalterschaltung 641 in einem Halbleitersubstrat CH40 oder CH42 gebildet, in der die Codeerzeugereinheit 400 zusammen mit der Verschlüsselungsschaltung 631, der Decodierschaltung 632 und der Schlüsselerzeugereinheit 633 gebildet ist. Die Umschalterschaltung 641 ist in einen Übertragungspfad des Identifikationscodes Cd#, der von der Verschlüsselungsschaltung 631 zu dem in einem Halbleitersubstrat CH41 gebildeten Speicher 601 übertragen wird, und einen Übertragungspfad des Speichercodes Co#, der von dem Speicher 601 zu der Decodierschaltung 632 übertragen wird, eingefügt und führt exklusiv die Übertragung des Identifikationscodes Cd# und die Übertragung des Speichercodes Co# durch.

[0287] Selbst wenn ein Benutzer einen Anschluß des Halbleitersubstrates CH40 (oder CH42) kurzschließt, so daß der Identifikationscode Cd#, der von der Verschlüsselungsschaltung 631 ausgegeben wird, direkt in die Decodierschaltung 632 eingegeben wird bei einem Versuch, eine betrügerische Benutzung durchzuführen, verhindert die Umschalterschaltung 641, daß der Identifikationscode Cd# direkt in die Decodierschaltung 632 eingegeben wird. Mit andern Worten, selbst wenn die betrügerische Benutzung durch Kurzschluß des Anschlusses versucht wird, ist es unmöglich vorzugeben, daß der Identifikationscode Cd und der Speichercode Co, die von der Komperatorschaltung 403 zu vergleichen sind, miteinander übereinstimmen. Somit kann die Halbleitervorrichtung 640 die betrügerische Benutzung des Gerätes durch Kurzschließen des Anschlusses des Halbleitersubstrates verhindern.

[0288] Ein anderer Aufbau, bei dem die Umschalterschaltung 641 zwischen der Codeerzeugereinheit 400 und der Verschlüsselungsschaltung 631 und zwischen der Komperatorschaltung 403 und der Decodierschaltung 632 eingefügt ist, kann den gleichen Effekt erzielen. Im allgemeinen muß die Umschalterschaltung 641 nur in den Übertragungspfad des Identifikationscodes Cd (Cd#) von der Codeerzeugereinheit 400 zu dem Speicher 601 und den Übertragungspfad des Speichercodes Co (Co#) von dem Speicher 601 zu der Komperatorschaltung 403 eingefügt werden.

[0289] Weiter kann die Umschalterschaltung 641 an die Halbleitervorrichtung 600 von Fig. 1 angewendet werden, die nicht die Verschlüsselungsschaltung 631 usw. aufweist. Insbesondere kann bei der Halbleitervorrichtung 600 von Fig. 1 die Umschalterschaltung 641 in dem Halbleitersubstrat CH1 (oder CH3) so gebildet werden, daß sie in den Übertragungspfad des Identifikationscodes Cd von der Codeerzeugereinheit

gereinheit 400 zu dem Speicher 601 und den Übertragungspfad des Speichercode Co von dem Speicher 601 zu der Komperatorschaltung 403 eingefügt ist. Dieses erzeugt den gleichen Effekt wie bei der Halbleitervorrichtung 640 von Fig. 30.

[0290] Weiter kann die Umschalterschaltung 641 auf die Halbleitervorrichtung 620 von Fig. 13 und auf die Halbleitervorrichtung 635 von Fig. 28 angewendet werden. Bei der Halbleitervorrichtung 620 von Fig. 13 wird die Umschalterschaltung 641 in den beiden Halbleitersubstraten CH4 (CH6) und CH5 gebildet. Bei der Halbleitervorrichtung 635 von Fig. 28 wird die Umschalterschaltung 641 in den beiden Halbleitersubstraten CH20 (oder CH22) und CH23 gebildet.

7. Siebte Ausführungsform

[0291] Die in dem Halbleiterelement 401 enthaltene Schlüsselerzeugereinheit 633, die bei der fünften Ausführungsform erörtert wurde, kann auf eine allgemeine Anschlußeinrichtung angewendet werden, die Daten von und zu einem Hostcomputer überträgt und empfängt. Die Anschlußeinrichtung mit solchem Aufbau wird bei der siebten Ausführungsform erörtert.

[0292] Fig. 31 ist ein Blockschaltbild, das einen Aufbau einer Anschlußeinrichtung gemäß der siebten Ausführungsform der vorliegenden Erfindung zeigt. Eine Anschlußeinrichtung 821 und ein damit verbundener Hostcomputer 825 stellen ein System 820 zum Übertragen und Empfangen von Daten Dd dazwischen dar. Die Anschlußeinrichtung 821 weist eine Dateneingangseinheit 822 zum Eingeben der Daten Dd und eine Datenausgangseinheit 823 zum Ausgeben der Daten Dd auf, sie weist weiter die Verschlüsselungsschaltung 631, die Decodierschaltung 632 und die Schlüsselerzeugereinheit 633 auf. Die Schlüsselerzeugereinheit 633 erzeugt den Schlüssel K zur Verschlüsselung. Die Verschlüsselungsschaltung 631 verschlüsselt die durch die Dateneingangseinheit 822 eingegebene Daten Dd in Daten Dd# auf der Grundlage des von der Schlüsselerzeugereinheit 633 erzeugten Schlüssels K und überträgt die Daten Dd# an den Hostcomputer 825.

[0293] Der Hostcomputer 825 speichert die verschlüsselten Daten Dd# in einem Speicher 826 als Daten Do#. Die Decodierschaltung 632 empfängt die in dem Speicher 826 gespeicherten Daten Do#, decodiert die Daten Do# in die Daten Dd auf der Grundlage des von der Schlüsselerzeugereinheit 623 erzeugten Schlüssels K und überträgt die Daten Dd an die Datenausgangseinheit 823. Die Daten Dd sind äquivalent zu den Daten Dd. Da somit die Anschlußeinrichtung 821 die verschlüsselten Daten zu und von dem Hostcomputer 825 überträgt und empfängt, ist die Barriere gegen das Lecken der Information, die durch die Daten dargestellt wird, hoch.

[0294] Der innere Aufbau der Schlüsselerzeugereinheit 623 ist in Fig. 26 gezeigt. Genauer, die Schlüsselerzeugereinheit 633 erzeugt den Schlüssel K der Anschlußeinrichtung inwohnend durch Benutzen der elektrischen Eigenschaft, die von einem Halbleiterelement 401 zu einem anderen variiert. Da es nicht notwendig ist den Schlüssel K bei dem Herstellungsvorgang der Anschlußeinrichtung 821 zu schreiben und die Halbleiterelemente 401, die durch den gleichen Vorgang hergestellt werden, als eine Menge von massenproduzierten Anschlußeinrichtungen 821 benutzt werden können, kann der Herstellungsvorgang der Anschlußeinrichtung 821 vereinfacht werden. Da weiter die elektrische Eigenschaft des Halbleiterelementes 401, auf der der Schlüssel K beruht, nicht von außen geändert werden kann, ist die Barriere gegen die betrügerische Änderung des Schlüssels K vorteilhafterweise hoch.

[0295] Fig. 32 ist ein Blockschaltbild, das einen anderen Aufbau der Anschlußeinrichtung gemäß der siebten Ausführungsform der vorliegenden Erfindung zeigt. Die Anschlußeinrichtung von Fig. 32 unterscheidet sich von der Anschlußeinrichtung 821 der Fig. 31 darin, daß die Schlüsselerzeugereinheit 633 in einer IC-Karte 829 eingebaut ist, die von einem Hauptkörperabschnitt 828 abnehmbar ist. Wenn die IC-Karte 829 an dem Hauptkörperabschnitt 828 angebracht ist, sind die Verschlüsselungsschaltung 631 und die Decodierschaltung 632, die in dem Hauptkörperabschnitt 828 gebildet sind, mit der Schlüsselerzeugereinheit 633 verbunden.

[0296] Da die Schlüsselerzeugereinheit 633 in der IC-Karte 829 enthalten ist, die von dem Hauptkörperabschnitt 828 abnehmbar ist, ist es möglich, den gleichen Schlüssel K für eine Mehrzahl von Hauptkörperabschnitten 828 zu benutzen, die voneinander entfernt eingebaut sind, in dem die tragbare IC-Karte 829 frei getragen werden kann.

8. Achte Ausführungsform

[0297] Bei der achten Ausführungsform wird eine Erörterung in Hinblick auf den Aufbau gegeben, in dem der Speicher 654, der den Speichercode Co speichert, in einen Hilfsabschnitt eingesetzt ist, der von einem Hauptkörperabschnitt in der Anschlußeinrichtung 801 der vierten Ausführungsform abnehmbar ist.

[0298] Fig. 33 ist ein Blockschaltbild, das einen Aufbau einer Anschlußeinrichtung gemäß der achten Ausführungsform der vorliegenden Erfindung zeigt. Die Anschlußeinrichtung ist in einem Hauptkörperabschnitt 651 und einem Batterieladegerät 653 als ein Hilfsabschnitt getrennt, die äquivalent ist zu einer Einrichtung, bei der ein Halbleitersubstrat CH50 in dem Hauptkörperabschnitt 651 enthalten ist und ein Halbleitersubstrat CH51 in dem Batterieladegerät 653 enthalten ist in der Anschlußeinrichtung 801 von Fig. 20. Der Hauptkörperabschnitt 651 weist eine wiederaufladbare Batterie auf, die nicht gezeigt ist, und das Batterieladegerät 653 lädt die Batterie auf, wenn es an dem Hauptkörperabschnitt 651 angebracht ist.

[0299] Wenn das Batterieladegerät 653 an dem Hauptkörperabschnitt 651 angebracht ist, wird nicht nur die Batterie geladen, sondern auch die Halbleitervorrichtung 652 mit dem Halbleitersubstrat CH50 ist mit dem Halbleitersubstrat CH51 verbunden. Die Kommunikationsschaltung 405a überträgt nur den Identifikationscode Cd aus dem Identifikationscode Cd und dem Speichercode Co zu der gemeinsamen Kommunikationsträgersausrüstung 655, wenn das Batterieladegerät nicht an dem Hauptkörperabschnitt 651 angebracht ist, und sie überträgt sowohl den Identifikationscode Cd als auch den Speichercode Co zu der gemeinsamen Kommunikationsträgersausrüstung 655, wenn das Batterieladegerät an dem Hauptkörperabschnitt 651 angebracht ist. Die gemeinsame Kommunikationsträgersausrüstung 655, der Hauptkörperabschnitt der Anschlußeinrichtung 651 und das Batterieladegerät 653 stellen ein Kommunikationssystem 650 dar.

[0300] Fig. 34 ist ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung von Fig. 33 zur Kommunikation. Zuerst wird die Halbleitervorrichtung 652 als ein Teil hergestellt (S501). Danach wird die Halbleitervorrichtung 652 an einen Telefonhersteller geliefert, und der Hauptkörperabschnitt 651 der Anschlußeinrichtung wird durch den Telefonhersteller zusammengesetzt (S502). Parallel zu diesen Schritten oder vor oder nach diesen Schritten wird der Speicher 654 als ein Teil hergestellt (S503), und das Batterieladegerät 653 wird danach von dem Telefonhersteller zusammengesetzt (S504).

[0301] Wenn sowohl der Hauptkörperabschnitt 651 der Anschlußeinrichtung als auch das Batterieladegerät 653 fertiggestellt sind, wird der Identifikationscode Cd in den Speicher 654 als der Speichercode Co geschrieben (S505), und ein Satz aus dem Hauptkörperabschnitt 651 der Anschlußeinrichtung und dem Batterieladegerät 653 wird für einen gemeinsamen Kommunikationsträger geliefert, der die gemeinsame Kommunikationsträgersausrüstung 655 trägt (S506). Sowohl der Identifikationscode Cd als auch der Speichercode Co werden in irgendeiner Stufe der Schritte S501 bis S506 ausgelesen und in dem Kundendatenbankspeicher 658 der gemeinsamen Kommunikationsträgersausrüstung 655 registriert (S507). Danach wird der Satz aus dem Hauptkörperabschnitt 651 der Anschlußeinrichtung und dem Batterieladegerät 653 an den Benutzer geliefert (S508) und dienen danach zur Kommunikation durch den Benutzer (S509).

[0302] Fig. 35 und 36 sind Flußdiagramme, die eine interne Prozedur des Schrittes S509 von Fig. 34 zeigen. Wenn die Kommunikation gestartet wird, wenn die Anschlußeinrichtung nicht zum Laden benutzt wird, mit andern Worten, wenn das Batterieladegerät 653 nicht an dem Hauptkörperabschnitt 51 angebracht ist (S520), überträgt der Hauptkörperabschnitt 651 der Anschlußeinrichtung den Identifikationscode Cd zu der gemeinsamen Kommunikationsträgersausrüstung 655 (S521). Die gemeinsame Kommunikationsträgersausrüstung 655 empfängt folglich den Identifikationscode Cd durch die Kommunikationsschaltung 656 (S522).

[0303] Darauf folgend vergleicht in der gemeinsamen Kommunikationsträgersausrüstung 655 die Beurteilungsschaltung 657 den Identifikationscode Cd mit dem registrierten Identifikationscode Cd und beurteilt, ob diese Codes miteinander übereinstimmen oder nicht, um das Freigabesignal En, das das Beurteilungsergebnis darstellt, an die Kommunikationsschaltung 656 zu übertragen (S523). Wenn das Freigabesignal En die Übereinstimmung der Codes anzeigt (S524), führt die gemeinsame Kommunikationsträgersausrüstung 655 eine Authentifikation durch, daß der Benutzer des Hauptkörperabschnittes 651 der Anschlußeinrichtung autorisiert ist, und wenn das Freigabesignal En Nichtübereinstimmung der Codes anzeigt (S524), führt die gemeinsame Kommunikationsträgersausrüstung 655 die Authentifikation nicht durch. Die gemeinsame Kommunikationsträgersausrüstung 655 erlaubt das Fortsetzen des Kommunikationsvorganges (S525), wenn die Authentifikation durchgeführt ist, und sie erlaubt nicht die Kommunikation zum Stoppen des Kommunikationsvorganges (S526), wenn die Authentifikation nicht durchgeführt ist.

[0304] Wenn die Anschlußeinrichtung zum Laden benutzt wird, mit andern Worten, wenn der Hauptkörperabschnitt 651 zur Kommunikation benutzt wird, während er mit dem Batterieladegerät 653 verbunden ist (S520, S530), überträgt der Hauptkörperabschnitt 651 der Anschlußeinrichtung sowohl den Identifikationscode Cd als auch den Speichercode Co zu der gemeinsamen Kommunikationsträgersausrüstung 655 (S531). Folglich empfängt die gemeinsame Kommunikationsträgersausrüstung 655 den Identifikationscode Cd und den Speichercode Co durch die Kommunikationsschaltung 656 (S532).

[0305] Darauf folgend vergleicht in der gemeinsamen Kommunikationsträgersausrüstung 655 die Beurteilungsschaltung 657 den Identifikationscode Cd mit dem registrierten Identifikationscode Cd zum Beurteilen, ob diese Codes miteinander übereinstimmen und vergleicht zur gleichen Zeit den Speichercode Co mit dem registrierten Speichercode Co zum Beurteilen, ob diese Codes miteinander übereinstimmen oder nicht. Die Beurteilungsschaltung 657 überträgt das Freigabesignal En, daß die zwei Beurteilungss-

resultate darstellt, an die Kommunikationsschaltung 656 (S533).

[0306] Wenn auf der Grundlage des Freigabesignales En erkannt wird, daß beide Beurteilungsergebnisse Übereinstimmung der Codes bezeichnen (S534), führt die gemeinsame Kommunikationsträgersausrüstung 655 eine Authentifikation durch, daß der Benutzer der Anschlußeinrichtung autorisiert ist, und wenn erkannt wird, daß mindestens einer der Beurteilungsergebnisse Nichtübereinstimmung der Codes bezeichnet (S534), führt die gemeinsame Kommunikationsträgersausrüstung 655 die Authentifikation nicht durch. Da die Beurteilung auf der Grundlage der beiden Codes Cd und Co in dem Schritt S533 durchgeführt wird, ist die Genauigkeit der Beurteilung in dem Schritt S533 höher als in dem Schritt S523. Mit andern Worten, die Authentifikation, die auf der Grundlage der Beurteilung in dem Schritt S533 durchgeführt wird, ist eine Hochniveauauthentifikation, die beweist, daß die Anschlußeinrichtung gültig benutzt wird, mit höherer Genauigkeit als die Authentifikation, die auf der Grundlage der Beurteilung in dem Schritt S523 durchgeführt wird.

[0307] Daher kann die gemeinsame Kommunikationsträgersausrüstung 655 selektiv die zwei Authentifikationen verschiedener Niveaus in Abhängigkeit von der Wichtigkeit benutzen. Als ein Beispiel, wenn die Authentifikation auf der Grundlage der Beurteilung in dem Schritt S533 durchgeführt wird, wenn die Anschlußeinrichtung für die Kommunikation benutzt wird (S535), ermöglicht die gemeinsame Kommunikationsträgersausrüstung 655 nicht nur, daß die Kommunikation den Kommunikationsvorgang fortsetzt (S536), sondern sie zeichnet auch die Kommunikationsladung für die Kommunikation davor (von der vorherigen Authentifikation auf der Grundlage der Beurteilung in dem Schritt S533 bis zu dieser Kommunikation) wie bestätigt auf, unabhängig davon, ob die Anschlußeinrichtung für die Kommunikation benutzt wird (S537). Es ist daher möglich, eine illegale Tätigkeit des Vermeidens der Pflicht des Zahlens unter dem Vorwand, daß die Anschlußeinrichtung verlorengegangen ist, zu verhindern. Da es ein seltener Fall ist, daß der Hauptkörperabschnitt 651 der Anschlußeinrichtung und das Batterieladegerät 653 zusammen verlorengehen, kann diese Bestätigung mit einer ausreichend hohen Genauigkeit gemacht werden.

[0308] Wenn weiter die Authentifikation nicht auf der Grundlage der Beurteilung in dem Schritt S533 durchgeführt wird, zeichnet die gemeinsame Kommunikationsträgersausrüstung 655 den Identifikationscode Cd und den Speichercode Co, die in dem Schritt S533 empfangen sind, in dem Kundendatenbankspeicher 658 getrennt von dem Identifikationscode Cd und dem Speichercode Co, die registriert worden sind, auf. Der aufgezeichnete Identifikationscode Cd und Speichercode Co können nützlich sein zum Spezifizieren des nichtautorisierten Benutzers.

[0309] Zurück zu Schritt S507 von Fig. 34, es kann einen anderen Fall geben, in dem nur der Identifikationscode Cd registriert ist anstelle der beiden des Identifikationscodes Cd und des Speichercode Co. In diesem Fall muß nur der Identifikationscode Cd in irgendeiner Stufe der Schritte S501 bis S506 ausgelesen werden. Das Registrieren des Speichercode Co wird erzielt durch Registrieren des Speichercode Co, der in dem Schritt S531 übertragen ist, in dem Kundendatenbankspeicher 658, wenn der Benutzer zum ersten Mal die Anschlußeinrichtung mit Aufladung benutzt (S530).

[0310] Weiter kann der Speicher 601 in einen Hilfsabschnitt eingesetzt werden, der nicht auf das Batterieladegerät 653 begrenzt ist, der von dem Hauptkörperabschnitt trennbar ist. Der Aufbau von Fig. 33, in dem der Hilfsabschnitt das Batterieladegerät 653 ist, weist jedoch den Vorteil der periodischen Verbindens des Hauptkörperabschnitt-

tes 651 und des Hilfsabschnittes, ohne eine extra Arbeit von dem Benutzer zu verlangen, auf.

9. Neunte Ausführungsform

[0311] Bei der neunten Ausführungsform wird die Erörterung über einen Aufbau gemacht, bei dem die Codes in verschlüsselter Form zwischen dem Hauptkörperabschnitt und dem Hilfsabschnitt und zwischen dem Hauptkörperabschnitt und der gemeinsamen Kommunikationsträgersausrüstung in der Anschlußeinrichtung der achten Ausführungsform übertragen werden.

[0312] Fig. 37 ist ein Blockschaltbild, das einen Aufbau einer Anschlußeinrichtung gemäß der neunten Ausführungsform der vorliegenden Erfindung zeigt. Die Anschlußeinrichtung unterscheidet sich von der Anschlußeinrichtung von Fig. 33 dadurch, daß die Verschlüsselungsschaltung 631 und die Schlüsselerzeugereinheit 633 in einer Halbleitervorrichtung 672 eines Hauptkörperabschnittes 671 gebildet sind und die Verschlüsselungsschaltung 631 und eine Schlüsselerzeugereinheit 676 ebenfalls in dem Batterieladegerät 653 gebildet sind. Folglich ist die Decodierschaltung 632 in einer gemeinsamen Kommunikationsträgersausrüstung 675 gebildet. Die gemeinsame Kommunikationsträgersausrüstung 675, der Hauptkörperabschnitt 671 der Anschlußeinrichtung und das Batterieladegerät 673 stellen ein Kommunikationssystem 670 dar.

[0313] In dem Batterieladegerät 673 erzeugt die Schlüsselerzeugereinheit 676 den Schlüssel K2 zur Verschlüsselung, und die Verschlüsselungsschaltung 631 verschlüsselt den Speichercode Co, der aus dem Speicher 601 gelesen ist, auf der Grundlage des Schlüssels K2 und überträgt den verschlüsselten Speichercode zu dem Hauptkörperabschnitt 671 als einen Speichercode Co#. In dem Hauptkörperabschnitt 671 erzeugt die Schlüsselerzeugereinheit 633 den Schlüssel K1 zur Verschlüsselung, und die Verschlüsselungsschaltung 631 verschlüsselt den durch die Codeerzeugereinheit 400 erzeugten Identifikationscode Cd auf der Grundlage des Schlüssels K1 und überträgt den verschlüsselten Identifikationscode zu der Kommunikationsschaltung 405a als einen Identifikationscode Cd#. Die Verschlüsselungsschaltung 631 in dem Hauptkörperabschnitt 671 verschlüsselt auch den von dem Batterieladegerät 673 übertragenen Speichercode Co# auf der Grundlage des Schlüssels K1 und überträgt den verschlüsselten Speichercode an die Kommunikationsschaltung 405a als einen Speichercode Co##. Der Speichercode Co## ist doppelt verschlüsselt auf der Grundlage der zwei Schlüssels K1 und K2.

[0314] Die Kommunikationsschaltung 405a überträgt den Identifikationscode Cd# und den Speichercode Co##, die verschlüsselt sind zu der gemeinsamen Kommunikationsträgersausrüstung 675. Die Decodierschaltung 632 der gemeinsamen Kommunikationsträgersausrüstung 675 decodiert den Identifikationscode Cd# und den Speichercode Co## in den Identifikationscode Cd und den Speichercode Co#, die für die Beurteilung in der Beurteilungsschaltung 657 dienen.

[0315] Da somit die Codes in der verschlüsselten Form zwischen dem Hauptkörperabschnitt 671 und dem Batterieladegerät 673 und zwischen dem Hauptkörperabschnitt 671 und der gemeinsamen Kommunikationsträgersausrüstung 675 in der Anschlußeinrichtung von Fig. 37 übertragen werden, ist die Barriere gegen das Lecken dieser Codes vorteilhafterweise hoch.

[0316] In dem Hauptkörperabschnitt 671 ist es bevorzugt, daß die Schlüsselerzeugereinheit 633 und die Verschlüsselungsschaltung 631 in dem einzelnen Halbleitersubstrat CH50 (oder CH50) zusammen mit der Codeerzeugereinheit 400 gebildet sind. Mit diesem Aufbau ist eine noch höhere

Barriere gegen das Lecken des Schlüssels K1 und des Identifikationscodes Cd erzielt. Ähnlich ist es in dem Batterieladegerät 673 bevorzugt, daß die Schlüsselerzeugereinheit 676 und die Verschlüsselungsschaltung 631 in einem einzelnen Halbleitersubstrat CH71 zusammen mit dem Speicher 654 gebildet sind. Mit diesem Aufbau wird eine noch höhere Barriere gegen das Lecken des Schlüssels K2 und des Speichercodes Co erzielt.

[0317] Fig. 38 ist ein Flußdiagramm einer Prozedur für die Benutzung der Anschlußeinrichtung von Fig. 37. Zuerst wird die Halbleitervorrichtung 672 als ein Teil hergestellt (S701). Danach wird die Halbleitervorrichtung 672 an einen Telefonhersteller geliefert, und der Hauptkörperabschnitt 671 der Anschlußeinrichtung wird von dem Telefonhersteller zusammengesetzt (S702). Parallel zu diesen Schritten oder vor oder nach diesen Schritten wird der Speicher 654 als ein Teil hergestellt (S703), und das Batterieladegerät 673 wird danach durch den Telefonhersteller zusammengesetzt (S704).

[0318] Wenn sowohl der Hauptkörperabschnitt 671 der Anschlußeinrichtung als auch das Batterieladegerät 673 fertiggestellt sind, wird der Identifikationscode Cd als der Speichercode Co in den Speicher 654 geschrieben (S705), und ein Satz aus einem Hauptkörperabschnitt 671 der Anschlußeinrichtung und dem Batterieladegerät 673 wird für einen gemeinsamen Kommunikationsträger geliefert, der die gemeinsame Kommunikationsträgersausrüstung 675 hält (S706). Der Identifikationscode Cd, der Speichercode Co# und der Schlüssel K1 werden in irgendeiner Stufe der Schritte S701 bis S706 ausgelesen und in dem Kundendatenbankspeicher 658 der gemeinsamen Kommunikationsträgersausrüstung 675 registriert (S707). Danach werden der Satz aus dem Hauptkörperabschnitt 671 der Anschlußeinrichtung und dem Batterieladegerät 673 an den Benutzer geliefert (S708) und dient danach zur Kommunikation durch den Benutzer (S709).

[0319] Fig. 39 und 40 sind Flußdiagramme, die eine interne Prozedur des Schrittes S709 von Fig. 38 zeigen. Wenn die Kommunikation gestartet wird, wenn die Anschlußeinrichtung nicht mit Aufladung benutzt wird, mit andern Worten, wenn das Batterieladegerät 673 nicht an dem Hauptkörperabschnitt 671 angebracht ist (S720), überträgt der Hauptkörperabschnitt 671 der Anschlußeinrichtung den Identifikationscode Cd# an die gemeinsame Kommunikationsträgersausrüstung 675 (S721). Folglich empfängt die gemeinsame Kommunikationsträgersausrüstung 675 den Identifikationscode Cd# an der Kommunikationsschaltung 656 (S722).

[0320] Darauf folgend decodiert in der gemeinsamen Kommunikationsträgersausrüstung 675 die Decodierschaltung 632 den Identifikationscode Cd# in den Identifikationscode Cd, und dann vergleicht die Beurteilungsschaltung 657 den Identifikationscode Cd mit dem registrierten Identifikationscode Cd und beurteilt, ob diese Codes miteinander übereinstimmen oder nicht, um das Freigabesignal En, das das Beurteilungsergebnis darstellt, an die Kommunikationsschaltung 656 zu übertragen (S723). Wenn das Freigabesignal En die Übereinstimmung der Codes anzeigt (S724), führt die gemeinsame Kommunikationsträgersausrüstung 675 eine Authentifikation durch, daß der Benutzer des Hauptkörperabschnittes 671 der Anschlußeinrichtung autorisiert ist, und wenn das Freigabesignal En die Nichtübereinstimmung der Codes anzeigt (S724), führt die gemeinsame Kommunikationsträgersausrüstung 675 die Authentifikation nicht durch. Die gemeinsame Kommunikationsträgersausrüstung 675 erlaubt der Kommunikation den Kommunikationsvorgang fortzuführen (S725), wenn die Authentifikation durchgeführt ist, und erlaubt die Kommunikation nicht zum

Stoppen des Kommunikationsvorganges (S726), wenn die Authentifikation nicht durchgeführt ist.

[0321] Wenn die Anschlußeinrichtung mit Aufladung benutzt wird, mit andern Worten, wenn der Hauptkörperabschnitt 671 zur Kommunikation benutzt wird, während er mit dem Batterieladegerät 673 verbunden ist (S720, S730), überträgt der Hauptkörperabschnitt 671 der Anschlußeinrichtung sowohl den Identifikationscode Cd# als auch den Speichercode Co## zu der gemeinsamen Kommunikationsladungs-ausrüstung 675 (S731). Folglich empfängt die gemeinsame Kommunikationsträgersausrüstung 675 den Identifikationscode Cd# und den Speichercode Co## durch die Kommunikationsschaltung 656 (S732).

[0322] Darauf folgend decodiert die Decodierschaltung 632 in der gemeinsamen Kommunikationsträgersausrüstung 675 den Identifikationscode Cd# in den Identifikationscode Cd und decodiert den Speichercode Co## in den Speichercode Co#, und dann vergleicht die Beurteilungsschaltung 675 den Identifikationscode Cd mit dem registrierten Identifikationscode Cd zum Beurteilen, ob diese Codes miteinander übereinstimmen oder nicht, und vergleicht zur gleichen Zeit den Speichercode Co# mit dem registrierten Speichercode Co# zum Beurteilen, ob diese Codes miteinander übereinstimmen oder nicht. Die Beurteilungsschaltung 675 überträgt das Freigabesignal En, daß die zwei Beurteilungsergebnisse darstellt, zu der Kommunikationsschaltung 656 (S733).

[0323] Wenn auf der Basis des Freigabesignales En erkannt wird, daß die Beurteilungsergebnisse die Übereinstimmung der Codes bezeichnen (S734), führt die gemeinsame Kommunikationsträgersausrüstung 675 eine Authentifikation durch, daß der Benutzer der Anschlußeinrichtung autorisiert ist, und wenn erkannt wird, daß mindestens eines der Beurteilungsergebnisse Nichtübereinstimmung der Codes bezeichnet (S734), führt die gemeinsame Kommunikationsträgersausrüstung 675 die Authentifikation nicht durch. Die auf der Grundlage der Beurteilung in dem Schritt S733 durchgeführte Authentifikation ist eine Hochniveaueuthentifikation, die vorsieht, daß die Anschlußeinrichtung gültig benutzt wird, mit höherer Genauigkeit als die Authentifikation, die auf der Beurteilung in dem Schritt S723 durchgeführt wurde.

[0324] Als ein Beispiel, wenn die Hochniveaueuthentifikation auf der Grundlage der Beurteilung in dem Schritt S733 durchgeführt wird, wenn die Anschlußeinrichtung für die Kommunikation benutzt wird (S735), erlaubt die gemeinsame Kommunikationsträgersausrüstung 675 nicht nur der Kommunikation den Kommunikationsvorgang fortzusetzen, sondern zeichnet auch die Kommunikationsladung für die Kommunikation davor auf (von der vorherigen Authentifikation auf der Grundlage der Beurteilung in dem Schritt S733 bis zu dieser Kommunikation), wie sie bestätigt wurde, unabhängig davon, ob die Anschlußeinrichtung für die Kommunikation benutzt wird (S737). Wenn weiter die Hochniveaueuthentifikation nicht auf der Grundlage der Beurteilung in dem Schritt S733 durchgeführt wird, zeichnet die gemeinsame Kommunikationsträgersausrüstung 675 den Identifikationscode Cd und den Speichercode Co, die in dem Schritt S732 empfangen sind, in dem Kundendatenbankspeicher 658 getrennt von dem Identifikationscode Cd und dem Speichercode Co auf, die registriert worden sind.

[0325] Zurück zu Schritt S707 von Fig. 38, es kann einen anderen Fall geben, in dem nur der Identifikationscode Cd und der Schlüssel K1 registriert sind anstelle des Identifikationscodes Cd, des Speichercodes Co# und des Schlüssels K1. In diesem Fall braucht nur der Identifikationscode Cd in irgendeiner Stufe der Schritt S701 bis S706 ausgelesen zu werden. Registrieren des Speichercodes Co# wird erzielt durch Registrieren des in dem Schritt S731 übertragenen

Speichercode Co# in den Kundendatenbankspeicher 658, wenn der Benutzer das erste Mal die Anschlußeinrichtung bei Aufladung benutzt (S730).

[0326] Somit kann durch Benutzung der Anschlußeinrichtung von Fig. 37 wie die Anschlußeinrichtung von Fig. 33 die gemeinsame Kommunikationsträgersausrüstung 675 selektiv die zwei Authentifikationen verschiedenen Niveaus in Abhängigkeit von der Wichtigkeit benutzen. Da weiter der Identifikationscode Cd und der Speichercode Co in der verschlüsselten Form übertragen werden, ist die Barriere gegen Lecken dieser Codes vorteilhafterweise hoch.

[0327] Es wird betrachtet, daß es einen Fall gibt, bei dem ein Austausch des Batterieladegerätes 673 notwendig ist, da das Batterieladegerät 673 verlorengegangen ist oder beschädigt ist. In solch einem Fall ist es bequem für den autorisierten Benutzer, wenn der Speichercode Co#, der registriert worden ist, in einen Speichercode Co# aktualisiert werden kann, der dem neuen Batterieladegerät 673 innewohnt/inhärent ist. Zum Aktualisieren des Speichercode Co# ist es nur notwendig, die Schritte S741 und S742 der Prozedur von Fig. 40 hinzuzufügen, wie in Fig. 41 gezeigt ist. In der Prozedur von Fig. 41, wenn der Speichercode Co# nicht geändert wird (S741), wird die Prozedur der Schritte S731 bis S738 wie bei der Prozedur von Fig. 40 durchgeführt, und wenn der Speichercode Co# geändert wird (S741), wird ein Änderungsvorgang des Speichercode Co#, der registriert ist, durchgeführt (S742).

[0328] Fig. 42 und 43 sind Flußdiagramme, die eine interne Prozedur des Änderungsvorganges (S742) von Fig. 41 zeigen. Wenn der Änderungsvorgang gestartet wird, werden der Identifikationscode Cd#, der Speichercode Co##, die Anschlußidentifikationsnummer und ein Anforderungssignal, das die Entscheidung des Änderns des registrierten Speichercode Co## darstellt, von der Anschlußeinrichtung zu der gemeinsamen Kommunikationsträgersausrüstung 675 übertragen (S752). Folglich empfängt die Kommunikationsträgersausrüstung 675 diese Codes, die Anschlußidentifikationsnummer und das Anforderungssignal an der Kommunikationsschaltung 656 (S753).

[0329] Darauf folgend decodiert die Decodierschaltung 632 in der gemeinsamen Kommunikationsträgersausrüstung 675 den Identifikationscode Cd# in den Identifikationscode Cd und decodiert den Speichercode Co## in den Speichercode Co#, und dann vergleicht die Beurteilungsschaltung 657 den Identifikationscode Cd mit dem registrierten Identifikationscode Cd und beurteilt, ob diese zwei Codes miteinander übereinstimmen oder nicht, und vergleicht den Speichercode Co# mit dem registrierten Speichercode Co# und beurteilt, ob diese Codes miteinander übereinstimmen oder nicht, und sie überträgt das Freigabesignal En, das die zwei Beurteilungsergebnisse darstellt, an die Kommunikationsschaltung 656 (S753).

[0330] Wenn auf der Grundlage des Freigabesignales En erkannt wird, daß die beiden Beurteilungsergebnisse die Übereinstimmung der Codes bezeichnen (S754), überträgt die gemeinsame Kommunikationsträgersausrüstung 675 die Nachricht der Erlaubnis zum Ändern des registrierten Speichercode Co# an die Anschlußeinrichtung und überträgt weiter eine Nachricht, die eine Änderung des Batterieladegerätes 673 in ein neues mit einem neuen Speichercode Co# verlangt, daß sie auf der Anzeigeeinrichtung angezeigt wird, wenn als Reaktion darauf ein Benutzer der Anschlußeinrichtung das Batterieladegerät 673 mit dem Speichercode Co# gegen ein neues Batterieladegerät 673 mit einem neuen Speichercode Co# (zur Vereinfachung der Erörterung als CoNeu# bezeichnet) tauscht (S757), werden der Identifikationscode Cd# und der Speichercode CoNeu## von der Anschlußeinrichtung zu der gemeinsamen Kommunikations-

trägerausrüstung 675 übertragen (S758). Folglich empfängt die gemeinsame Kommunikationsträgerausrüstung 675 diesen Identifikationscode Cd# und den Speichercode CoNeu## an der Kommunikationsschaltung 656 (S753).

[0331] Darauf folgend decodiert in der gemeinsamen Kommunikationsträgerausrüstung 675 die Decodierschaltung 632 den Identifikationscode Cd# in den Identifikationscode Cd und decodiert den Speichercode CoNeu## in den Speichercode CoNeu# (S760). Danach aktualisiert die gemeinsame Kommunikationsträgerausrüstung 675 den Speichercode Co#, der in dem Kundendatenbankspeicher 658 registriert ist, in den Speichercode CoNeu#.

[0332] Wenn auf der Grundlage des Freigabesignales En erkannt wird, daß mindestens eines der Beurteilungsergebnisse eine Nichtübereinstimmung der Codes anzeigt (S754), führt die gemeinsame Kommunikationsträgerausrüstung 675 nicht weiter den Änderungsvorgang durch und überträgt eine Nachricht, die einen neuen Versuch mit dem gegenwärtig benutzten Batterieladegerät 673 anregt, die auf der Anschlußeinrichtung anzuzeigen ist (S755).

[0333] Der gleiche Änderungsvorgang wie der Schritt S742 kann nicht nur zu der in Fig. 40 gezeigten Prozedur, sondern auch zu der in Fig. 36 gezeigten Prozedur hinzugefügt werden, bei der keine Verschlüsselung benutzt wird. Dieses erlaubt dem Benutzer, das Batterieladegerät 653 von Fig. 33 auszuwechseln.

[0334] Anstatt der Benutzung des OTPROM für den Speicher 654 in dem Batterieladegerät 653 und 673 kann ein wiederbeschreibbarer Speicher wie ein Flash-ROM benutzt werden. Der obige Änderungsvorgang S742 ist auch für die Benutzung des Batterieladegerätes 653 und 673 geeignet, bei der der Speichercode Co# neu geschrieben werden kann. Für eine höhere Sicherheit gegen die betrügerische Änderung ist es auch möglich, den Änderungsvorgang des registrierten Speichercode Co# auf einen Fall zu begrenzen, bei dem die Anschlußeinrichtung eine Information zum Sicherstellen von Ladungen wie eine Kreditkartennummer überträgt.

[0335] Fig. 44 und 45 sind Flußdiagramme, die einen anderen internen Fluß des Kommunikationsvorganges (S709) von Fig. 38 zeigen. Bei dem Kommunikationsvorgang (S770) wird die Authentifikation für eine Geschäftstätigkeit benutzt. Insbesondere wenn die Hochniveauauthentifikation auf der Grundlage der Beurteilung in dem Schritt S733 ausgeführt wird, wenn die Anschlußeinrichtung für Kommunikation benutzt wird (S735), setzt die gemeinsame Kommunikationsträgerausrüstung 675 den Kommunikationsvorgang fort zum Ermöglichen der Geschäftstätigkeit (S774) und zeichnet weiter die Geschäftstätigkeit in der Kombination davor auf (von der vorherigen Authentifikation auf der Grundlage in dem Schritt S733 bis zu dieser Kommunikation, wie sie abgeschlossen wurde, unabhängig davon, ob die Anschlußeinrichtung für Kommunikation benutzt wird (S775)). Wenn andererseits die Hochniveauauthentifikation nicht durchgeführt wird auf der Grundlage der Beurteilung in dem Schritt S733, zeichnet die gemeinsame Kommunikationsträgerausrüstung 675 die Geschäftstätigkeit in der Kommunikation davor als nicht abgeschlossen auf (S776).

[0336] Mit der Aufzeichnung, daß die Geschäftstätigkeit abgeschlossen ist auf der Grundlage der hochgenauen Authentifikation, kann ein Handelspartner verschiedene Prozeduren durchführen wie die Versendung von Produkten, da die Geschäftstätigkeit auf der Grundlage der Aufzeichnung gültig ist, und mit der Aufzeichnung, daß die Geschäftstätigkeit nicht abgeschlossen ist, kann der Handelspartner die Prozedur für die Geschäftstätigkeit stoppen. Dieses macht es möglich, den Verlust durch illegale Geschäftstätigkeiten aufzulösen oder zu verringern, die durch betrügerische Be-

nutzung der Anschlußeinrichtung verursacht wird.

[0337] Bevorzugter, wenn die Hochniveauauthentifikation nicht auf der Grundlage der Beurteilung in dem Schritt S733 ausgeführt wird, macht die gemeinsame Kommunikationsträgerausrüstung 675 eine Aufzeichnung so, daß die Geschäftstätigkeit nicht im Auftrag nicht erlaubt wird (S777). Die Aufzeichnung wird zum Beispiel durch Setzen eines Flag in einem Register eines Computersystemes der gemeinsamen Kommunikationsträgerausrüstung 675 durchgeführt.

[0338] Wenn die Anschlußeinrichtung nicht für Aufladung benutzt wird, mit andern Worten, wenn das Batterieladegerät 673 nicht an dem Hauptkörperabschnitt 671 angebracht ist (S720), wenn die Authentifikation auf der Grundlage der Beurteilung des Schrittes S723 durchgeführt wird, wird beurteilt, ob das Aufzeichnen, die Geschäftstätigkeit nicht zu erlauben ohne Aufladung, gemacht ist oder nicht (z. B. ob das obige Flag gesetzt ist oder nicht) (S771). Wenn die obige Aufzeichnung nicht gemacht ist, fährt die gemeinsame Kommunikationsträgerausrüstung 675 den Kommunikationsvorgang fort zum Erlauben der Geschäftstätigkeit (S772), und wenn die Aufzeichnung gemacht ist, stoppt die gemeinsame Kommunikationsträgerausrüstung 675 den Kommunikationsvorgang (S773).

[0339] Da das hochgenaue Beurteilungsergebnis, das in der Vergangenheit durchgeführt wurde, auf die normale Authentifikation reflektiert wird, die durchgeführt wird, wenn das Batterieladegerät 673 nicht an dem Hauptkörperabschnitt 671 angebracht ist, ist es möglich, eine wichtige Prozedur wie eine Geschäftstätigkeit unter der normalen Authentifikation durchzuführen. Weiterhin können die Schritte S772 bis S773 und S774 bis S777, die in Fig. 44 und 45 gezeigt sind, in dem Schritt S509 ausgeführt werden, der in Fig. 35 und 36 gezeigt ist.

[0340] Das Batterieladegerät 673 von Fig. 37 kann durch eine tragbare IC-Karte ersetzt werden. In diesem Fall muß der Benutzer manchmal die IC-Karte an dem Hauptkörperabschnitt 671 anbringen, aber wenn der Speichercode Co# von der IC-Karte zu dem Hauptkörperabschnitt 671 drahtlos übertragen werden kann, ist es möglich, die Mühe des Benutzers des Anbringens der IC-Karte an dem Hauptkörperabschnitt 671 zu sparen zum Zwecke der Bequemlichkeit des Benutzers. Fig. 46 ist ein Blockschaltbild, das einen anderen Aufbau der Anschlußeinrichtung zum Erzielen der obigen Funkverbindung zeigt.

[0341] In der Anschlußeinrichtung von Fig. 46 ist eine Kommunikationsschnittstelle 694 in einer Halbleitervorrichtung 692 eines Hauptkörperabschnittes 691 vorgesehen, und eine Kommunikationsschnittstelle 195 ist in einer IC-Karte 693 vorgesehen. Die Kommunikationsschnittstelle 694 ist in einem einzelnen Halbleitersubstrat CH90 (oder CH91) zusammen mit der Schlüsselerzeugereinheit 633, der Verschlüsselungsschaltung 631 und der Codeerzeugereinheit 400 gebildet. Ähnlich ist die Kommunikationsschnittstelle 695 in einem einzelnen Halbleitersubstrat CH92 zusammen mit der Schlüsselerzeugereinheit 676, der Verschlüsselungsschaltung 631 und dem Speicher 654 gebildet.

[0342] Die Kommunikationsschnittstellen 694 und 695 sind Schnittstellen für Funkkommunikation gemäß dem Bluetooth-Standard zum Beispiel. Daher wird der Speichercode Co# von der IC-Karte 693 zu dem Hauptkörperabschnitt 691 durch Funkkommunikation übertragen. Aus diesem Grund ist es möglich, selbst wenn die IC-Karte 693 in der Tasche einer Jacke des Benutzers ist und der Hauptkörperabschnitt 691 in einer Tasche ist, die von dem Benutzer getragen wird, sowohl den Identifikationscode Cd# und den Speichercode Co## zu der gemeinsamen Kommunikationsträgerausrüstung 675 zu übertragen. Anstelle der IC-Karte

693 kann eine Karte wie ein UIM (Universalteilnehmeridentifikationsmodul), das in den Hauptkörperabschnitt eines Mobiltelefones eingeführt wird, wenn es benutzt wird, benutzt werden. In diesem Fall jedoch ist es bevorzugter, da eine Möglichkeit des Verlierens sowohl des Hauptkörperabschnittes als auch der Karte zu der gleichen Zeit betrachtet werden sollte, daß der Speichercode Co# zwischen dem Hauptkörperabschnitt und einem getrennten unabhängigen Gerät übertragen wird, wie in Fig. 46 gezeigt ist.

[0343] Weiter kann in dem Kommunikationssystem 670 die gemeinsame Kommunikationsträgersausrüstung 675 durch ein ATM-System einer Bank oder andere gemeinsame Kommunikationsträgersausrüstungen ersetzt werden, wie in Fig. 12 gezeigt ist. Wenn zum Beispiel eine Geschäftstätigkeit auf der Grundlage der Authentifikation durchgeführt wird, kann das ATM-System der Bank, die ein Handelspartner der Anschlußeinrichtung ist, Direktprozeduren wie Identifikation, Erlaubnis der Geschäftstätigkeit und Nichterlaubnis durchführen. Das gleiche trifft für das Kommunikationssystem anderer vorliegender Ausführungsform zu.

10. Zehnte Ausführungsform

[0344] Es hat ein Problem gegeben, daß die Anschlußeinrichtung die Funkverbindung durch die gemeinsame Kommunikationsträgersausrüstung nicht ausführen kann in einem Bereich, in dem Funkwellen Schwierigkeiten einzudringen, z. B. ein unterirdisches Einkaufsgebiet oder Gebäude. Zum Ermöglichen der Funkverbindung in solch einem Bereich ist es notwendig, eine Menge von Basisstationen aufzustellen. Bei der zehnten Ausführungsform wird die Erläuterung für eine Anschlußeinrichtung und ein Kommunikationsverfahren gegeben, daß die Funkkommunikation ohne eine Basisstation selbst in einem Bereich ermöglicht, in dem die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung nicht ausgeführt werden kann. Bei der Anschlußeinrichtung des Kommunikationsverfahrens dieser Ausführungsform sind die Verschlüsselungsschaltung, die Decodierschaltung und die Schlüsselerzeugereinheit, die bei der fünften Ausführungsform beschrieben wurden, nützlich.

10.1. Umriß

[0345] Fig. 47 ist ein erläuterndes Bild eines Kommunikationsverfahrens gemäß der zehnten Ausführungsform der vorliegenden Erfindung. Bei diesen Verfahren wird eine Anschlußeinrichtung benutzt, die sowohl eine Funkverbindung durch eine gemeinsame Kommunikationsträgersausrüstung als auch durch ein Funkkommunikationsnetzwerk ohne die gemeinsame Kommunikationsträgersausrüstung bilden kann. Bei einem unten erörterten Beispiel wird ein drahtloses lokales Netz (LAN) als das Funkkommunikationsnetzwerk benutzt. Selbst in einem Bereich, in dem Funkwellen schwierig eindringen können, sammeln sich Menschen in Mengen oder gehen vorbei. Heutzutage tragen die meisten solcher Leute Mobiltelefone. Wenn die Mobiltelefone, die die Leute tragen, Anschlußeinrichtungen mit der obigen Funktion sind, wie in Fig. 47 gezeigt ist, wird das drahtlose LAN unter einer Mehrzahl von Anschlußeinrichtungen 140a bis 140d gebildet, wodurch eine gegenseitige Kommunikation ermöglicht wird. Zum Beispiel benutzen die Anschlußeinrichtungen 840a und 840d die Anschlußeinrichtungen 840b und 840c als Relais, wodurch die gegenseitige Kommunikation ermöglicht wird.

[0346] Als das drahtlose LAN kann eines in Übereinstimmung mit dem Bluetooth-Standard benutzt werden. In diesem Fall kann eine Anschlußeinrichtung eine Kombination drahtlos mit einer anderen Anschlußeinrichtung innerhalb

eines Bereiches eines 10 Meter Radius um es selbst ausführen. In einem unterirdischen Einkaufsgebiet oder -gebäude sind eine Menge von Passanten, Arbeitern und ähnliches normalerweise innerhalb eines Bereiches eines 10 Meter Radius vorhanden, und durch die Anschlußeinrichtungen, die diese Leute tragen, kann eine Kommunikation, die gesamt das unterirdische Einkaufsgebiet oder -gebäude abdeckt, erzielt werden.

[0347] Die Benutzung des drahtlosen LAN macht vorteilhafterweise den Betrieb mit kleiner Leistung möglich. Zum Beispiel beträgt der Leistungsverbrauch des drahtlosen LAN, das den Bereich eines 10 Meter Radius abdeckt, der nötig für die Funkwellen ist, etwa $(1/100)^2$ einer Funkkommunikation, die den Bereich von einem 1 Kilometer Radius abdeckt. Wenn tausend Anschlußeinrichtungen, die in 1 Meter Intervallen im Durchschnitt ausgerichtet sind, die Kommunikation fortpflanzend zum Herstellen der Kommunikation zwischen den Anschlußeinrichtungen, die 1 Kilometer getrennt sind, wird der gesamte Leistungsverbrauch auf $(1/100)^2 \times 1000 = 1/10$ der der obigen Funkkommunikation verringert.

[0348] Weiter kann nicht nur in dem Bereich, in dem Funkwellen schwierig eindringen können, wie ein unterirdisches Einkaufsgebiet oder -gebäude, sondern auch in einem Raum, in dem sich Menschen im allgemeinen in Mengen sammeln, vorbeikommen oder leben, die Kommunikation durch andere Anschlußeinrichtungen durch Bilden des drahtlosen LAN erzielt werden. Selbst wenn der Raum einen Bereich enthält, in den die Funkwellen schwierig eindringen können, wie ein Untergrundeinkaufsgebiet oder -gebäude, ist die Kommunikation durch andere Anschlußeinrichtungen nicht blockiert. Wenn weiter die Anschlußeinrichtungen in Häusern das drahtlose LAN als Relais benutzen, kann eine Architektur eines Funkkommunikationssystems mit niedrigem Leistungsverbrauch, das praktische keine Basisstationen benötigt, in Wohnblöcken auf der Erde erzielt werden.

10.2. Beispiel einer Anschlußeinrichtung

[0349] Bei der Kommunikation durch das in Fig. 47 gezeigte drahtlose LAN ist es notwendig, die Sicherheit gegen Lecken des Kommunikationsinhaltes sicherzustellen, da die Kommunikation durch die Anschlußeinrichtungen durchgeführt wird, die eine unspezifizierte Zahl von Personen trägt. Zum Sicherstellen der Sicherheit braucht die Anschlußeinrichtung 840 nur einen Aufbau aufzuweisen, bei dem ein Abschnitt für Funkkommunikation durch eine gemeinsame Kommunikationsträgersausrüstung (zeitweilig als Fernverkehrseinheit bezeichnet) 847 und ein Abschnitt für die Kommunikation durch das drahtlose LAN (zeitweilig als eine Nahverkehrseinheit bezeichnet) 848 elektrisch getrennt sind, wie in Fig. 48 gezeigt ist.

[0350] Die Fernverkehrseinheit 847 weist eine Kommunikationsschaltung 841 zum Durchführen der Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung, ein Mikrofon 842 zum Eingeben der Stimme, einen Lautsprecher 843 zum Ausgeben der Stimme, eine Eingangseinheit 845 zum Eingeben von Wählzahlen und ähnliches durch Tastentätigkeiten und ähnliches und eine Anzeigetafel 844 zum Anzeigen von Information mit Buchstaben, Zeichen, Grafiken und ähnliches auf. Die Nahverkehrseinheit 848 weist eine drahtlose LAN-Schaltung 846 zum Bilden eines drahtlosen LAN zum Durchführen der Funkverbindung auf. Da die Fernverkehrseinheit 847 und die Nahverkehrseinheit 848 voneinander in einer Anschlußeinrichtung 840 von Fig. 48 getrennt sind, kann ein Benutzer, der die Anschlußeinrichtung 840 trägt, keine Kommunikation

durch das drahtlose LAN ausführen sondern nur die Kommunikation anderer weiterleiten.

[0351] Zum Ermöglichen für den Benutzer, der die Anschlußeinrichtung trägt, die Kommunikation durch das drahtlose LAN durchzuführen, und zum Sicherstellen der Sicherheit gegen das Lecken des Kommunikationsinhaltes, kann eine Verschlüsselungstechnik benutzt werden, wie in Fig. 49 gezeigt ist. Selbst wenn die Funkkommunikation durch die gemeinsame Kommunikationsträgersausrüstung eine Verschlüsselungstechnik benutzt, benutzt die Funkkommunikation durch das drahtlose LAN seine eigene Verschlüsselungstechnik unterschiedlich davon.

[0352] Zwischen der drahtlosen LAN-Schaltung 846 und der Kommunikationsschaltung 841 ist ein Übertragungspfad des Kommunikationssignales vorgesehen, und eine Auswahlerschaltung 856, eine Verschlüsselungsschaltung 851 und eine Decodierschaltung 852 sind in diesen Übertragungspfad eingefügt. Die Auswahlerschaltung 856 verbindet und trennt selektiv den obigen Übertragungspfad. Wenn die Auswahlerschaltung 856 den obigen Übertragungspfad verbindet, ist die Kommunikation durch das drahtlose LAN hergestellt zwischen dem Benutzer einer Anschlußeinrichtung 850 und einer anderen Person. Wenn die Auswahlerschaltung 856 den obigen Übertragungspfad trennt, leitet die Anschlußeinrichtung 850 nur die Kommunikation anderer Personen durch das drahtlose LAN weiter. Obwohl die Antennen in eine für die Übertragung und eine für den Empfang in Fig. 49 getrennt sind zum Erleichtern der Darstellung, wird normalerweise eine einzelne Antenne gemeinsam benutzt.

[0353] Die Verschlüsselungsschaltung 851, die Decodierschaltung 852 und die Schlüsselerzeugungseinheit 853 führen ihre eigenen Funktionen durch zum Herstellen der Kommunikation durch das drahtlose LAN zwischen dem Benutzer der Anschlußeinrichtung 850 und einer anderen Person, wenn die Auswahlerschaltung 856 den obigen Übertragungspfad schließt. Die Schlüsselerzeugungseinheit 853 erzeugt den Schlüssel K zur Verschlüsselung. Die Verschlüsselungsschaltung 851 verschlüsselt ein Übertragungssignal, das von der Kommunikationsschaltung 841 zu einer Senderschaltung 855 der drahtlosen LAN-Schaltung 846 übertragen wird auf der Grundlage des Schlüssels K. Die Decodierschaltung 852 decodiert ein empfangenes Signal, das von einer Empfangerschaltung 854 der drahtlosen LAN-Schaltung 846 zu der Kommunikationsschaltung 841 übertragen ist, auf der Grundlage des Schlüssels K.

[0354] In diesem Fall muß der Schlüssel K ein Schlüssel sein, der mit dem Partner der Kommunikation, die die Anschlußeinrichtung durch das drahtlose LAN durchführt, geteilt wird. Aus diesem Grund weist die Schlüsselerzeugungseinheit 853 einen internen Aufbau auf, wie er in Fig. 50 gezeigt ist. Genauer, die Schlüsselerzeugungseinheit 853 weist die Codeerzeugungseinheit 633 und eine Schlüsselberechnungseinheit 857 auf. Die Codeerzeugungseinheit 633 erzeugt einen Identifikationscode, der der Anschlußeinrichtung 850 innewohnt/inhärent ist. Die Schlüsselberechnungseinheit 857 berechnet einen geteilten Schlüssel, der zwischen dem Benutzer der Anschlußeinrichtung 850 und dem Kommunikationspartner geteilt wird, auf der Grundlage eines anderen Codes, der von dem Kommunikationspartner durch die drahtlose LAN-Schaltung 846 übertragen wird, und gibt den geteilten Schlüssel als den Schlüssel K aus.

[0355] Es ist wünschenswert, daß die Codeerzeugungseinheit 633 den Aufbau von Fig. 25 oder 26 in der fünften Ausführungsform hat. Dieses erzeugt den gleichen Effekt wie bei der fünften Ausführungsform. Fig. 50 stellt ein Beispiel dar, bei dem die Codeerzeugungseinheit 633 den Aufbau von Fig. 26 aufweist.

10.3. Prozedur der Schlüsselerzeugung

[0356] Fig. 51 ist ein Flußdiagramm, das eine beispielhafte Prozedur zum Erzeugen des Schlüssels K durch die Schlüsselerzeugungseinheit 853 zeigt. Die Prozedur von Fig. 51 benutzt das gut bekannte DH-Verfahren. Wenn die Kommunikation durch das drahtlose LAN gestartet wird zwischen der Anschlußeinrichtung 850 und einer anderen Anschlußeinrichtung, wird beurteilt, ob die andere Anschlußeinrichtung, d. h. der Kommunikationspartner einer erstmaliger Partner ist oder nicht (S801). Wenn der Kommunikationspartner ein erstmaliger ist, wird ein Code $\alpha\# = g^{\alpha} \bmod(p)$ durch die Schlüsselerzeugungseinheit 837 auf der Grundlage einer vorbestimmten Primzahl p und einer vorbestimmten natürlichen Zahl g berechnet. In diesem Fall stellt α den Identifikationscode Cd dar, der von der Codeerzeugungseinheit 633 erzeugt wird, $\bmod()$ stellt einen Modulus in der Zahlentheorie dar, und die Primzahl p und die natürliche Zahl g sind allen Anschlußeinrichtungen gemeinsam, die öffentlichen Schlüsseln entsprechen.

[0357] Darauf folgend wird der berechnete Code $\alpha\#$ durch die Kommunikationsschaltung 841 und die Senderschaltung 855 zu dem Kommunikationspartner übertragen (S803). Dann wird ein Code $\beta\# = g^{\beta} \bmod(p)$ von der ersten Empfangerschaltung 854 empfangen und durch die Kommunikationsschaltung 841 zu der Schlüsselberechnungseinheit 857 übertragen (S804). Die Schlüsselberechnungseinheit 857 berechnet den Schlüssel $K = g^{\alpha\beta} \bmod(p)$ (S805). Danach zeichnet die Schlüsselberechnungseinheit 857 den berechneten Schlüssel K in einem Speicher 858 mit einer Identifikationsnummer (z. B. Telefonnummer) des Kommunikationspartners auf (S806).

[0358] Als nächstes liefert die Schlüsselberechnungseinheit 857 den Schlüssel K an die Verschlüsselungsschaltung 851 und die Decodierschaltung 852 zum Herstellen einer Chiffrekommunikation, wobei der Schlüssel K als geteilter Schlüssel benutzt wird (S808). Der Vorgang des Schrittes S808 setzt sich fort, bis die Kommunikation zu Ende ist (S809). In dem Schritt S801, wenn beurteilt wird, daß der Kommunikationspartner nicht der erstmalige ist, berechnet die Schlüsselberechnungseinheit 857 nicht den Schlüssel K, sondern liest den Schlüssel K aus dem Speicher 858 (S807), und dann werden die Vorgänge der Schritte S808 und S809 ausgeführt. Die Beurteilung in dem Schritt S801 kann auf der Grundlage gemacht werden, ob die Aufzeichnung in dem Speicher 858 gefunden wird oder nicht.

[0359] Somit kann, da die Chiffrekommunikation auf der Grundlage des geteilten Schlüssels durchgeführt wird, die durch das Austauschen der Identifikationscodes mit dem Kommunikationspartner erzeugt wird, die Kombination mit irgendeinem Kommunikationspartner hergestellt werden, wobei das Lecken des Kommunikationsinhaltes verhindert wird. Weiter kann es in der Prozedur von Fig. 51 ein anderes Beispiel geben, bei dem die Schritte S801 und S807 weggelassen werden, und der Schlüssel K jedes Mal berechnet wird, wenn die Kommunikation durchgeführt wird.

10.4. Anderes Beispiel der Anschlußeinrichtung

[0360] Fig. 52 ist ein Blockschaltbild, das einen anderen Aufbau der Anschlußeinrichtung gemäß der zehnten Ausführungsform der vorliegenden Erfindung zeigt. Bei dieser Anschlußeinrichtung 860 wird ein Empfangssignal, das von einer Kommunikationsschaltung 861 empfangen wird, durch einen Niederfrequenzverstärker 842 verstärkt und von einem Mischer 863 demoduliert, der mit einem VCO (spannungsgesteuerter Oszillator) 864 gekoppelt ist, und dann von einer Basisbandschaltung 878 verarbeitet. Weiter wird

ein Übertragungssignal, das von der Basisbandschaltung **878** verarbeitet ist, von einem Mischer **865** moduliert, der mit einem VCO **866** gekoppelt ist, und von einem Leistungsverstärker **867** verstärkt und dann zu der gemeinsamen Kommunikationsträgerschaltung übertragen.

[0361] Andererseits wird ein von einem drahtlosen LAN **871** empfangenes Empfangssignal von einem rauscharmen Verstärker **872** verstärkt und von einem Mischer **873** demoduliert, der mit einem VCO **874** gekoppelt ist, wobei es durch eine Auswahlhaltung **870** geht, dann von einem Mischer **868** moduliert, der mit einem VCO **869** gekoppelt ist. Das modulierte Empfangssignal geht durch den Mischer **863** in der Kommunikationsschaltung **861** und wird an die Basisbandschaltung **878** eingegeben. Das empfangene Signal von der drahtlosen LAN, das an die Basisbandschaltung **878** eingegeben ist, wird von der Decodierschaltung **852** demoduliert. Ein Übertragungssignal des drahtlosen LAN geht durch die Basisbandschaltung **878**, die Verschlüsselungsschaltung **851** und die Auswahlhaltung **870** und wird dann an eine Basisbandschaltung **879** eingegeben. Danach wird das Übertragungssignal von einem Mischer **875** moduliert, der mit einem VCO **766** gekoppelt ist, und von einem Leistungsverstärker **877** verstärkt und dann übertragen.

[0362] Somit wird in der Anschlußeinrichtung **860** von Fig. 52 das Empfangssignal, das an die drahtlose LAN-Schaltung **871** angelegt wird, demoduliert und danach moduliert und an die Kommunikationsschaltung **861** eingegeben. Wie in Fig. 53 gezeigt ist, moduliert der Mischer **853** das demodulierte Empfangssignal des drahtlosen LAN mit einer Trägerwelle mit einer Frequenz f innerhalb eines angegebenen Bereiches (als "Spezialband" in Fig. 53 dargestellt) in einem Kommunikationsschaltungsband. Daher wird, in welchem Bereich eines drahtlosen LAN-Bandes die Frequenz f des Empfangssignales des drahtlosen LAN auch immer existiert, eine modulierte Welle, deren Frequenz f in dem Spezialband vorhanden ist, an die Kommunikationsschaltung **861** eingegeben.

[0363] Es sei angenommen, das Empfangssignal des drahtlosen LAN wird nicht demoduliert sondern in die Kommunikationsschaltung **861** eingegeben, wobei nur seine Frequenz umgewandelt wird, es wird notwendig, ein weiteres Kommunikationsschaltungsband sicherzustellen, wie in Fig. 54 gezeigt ist. Im Gegensatz dazu ist es bei der Anschlußeinrichtung **860** von Fig. 52 nicht notwendig, ein breites Kommunikationsschaltungsband vorzusehen, und daher kann das Benutzungsverhältnis des Frequenzbandes der Kommunikationsschaltung **861** vorteilhafterweise verbessert werden.

[0364] Bei der Anschlußeinrichtung, bei der die Kommunikationsschaltung und die drahtlose LAN-Schaltung selektiv kombiniert werden, wie in Fig. 49 oder 52 dargestellt ist, wird es möglich, den Kommunikationspfad durch die gemeinsame Kommunikationsträgerschaltung und das drahtlose LAN zu kombinieren, wie in Fig. 55 gezeigt ist. Genauer, durch die Kommunikationsschaltung in der Fernverkehrseinheit **847** der Anschlußeinrichtung **850c**, die eine einer Mehrzahl von Anschlußeinrichtungen **850a** bis **850c** darstellt, die ein drahtloses LAN bilden, kann eine andere Anschlußeinrichtung **850a** eine Kommunikation durch die gemeinsame Kommunikationsträgerschaltung durchführen. Es ist auch möglich für eine Anschlußeinrichtung in einem unterirdischen Einkaufsgebiet, in dem die Funkwelle Schwierigkeiten beim Eintreten hat, eine Kommunikation durch die gemeinsame Kommunikationsträgerschaltung durchzuführen. Zum Verringern der Last der Anschlußeinrichtung, die den Kommunikationspfad durch die gemeinsame Kommunikationsträgerschaltung und das drahtlose

LAN kombiniert (die Anschlußeinrichtung **850c** in dem Beispiel von Fig. 55) sollte solch eine Kommunikation nur für Notfallkommunikation erlaubt werden.

[0365] Weiter ist es möglich, die gesamte Kommunikation durch das drahtlose LAN auf Notfallkommunikation zu begrenzen. Dieses verringert die Last der Anschlußeinrichtungen, die die Kommunikation durch das drahtlose LAN weiterleiten (die Anschlußeinrichtungen **840b** und **840c** in dem Beispiel von Fig. 47). Da die Wichtigkeit der Sicherheit gegen Lecken des Kommunikationsinhaltes in der Notfallkommunikation niedrig ist, ist es möglich, die Schaltungen für die Verschlüsselung zu entfernen. Die Notfallkommunikation bezieht sich auf eine Kommunikation zum Anfordern von Hilfe, zu einer Zeit, wenn ein Notfall auftritt, der eine Gefahr für Leib und Eigentum darstellt.

11. Elfte Ausführungsform

[0366] Selbst in einem Gebiet, in dem sich normalerweise Menschen in Mengen konzentrieren, wie ein unterirdisches Einkaufsgebiet und -gebäude kann die Bevölkerungsdichte in Abhängigkeit von der Zeit, zum Beispiel bei Nacht niedrig werden. Bei der elften Ausführungsform wird eine Erörterung über ein Verfahren gegeben zum Ermöglichen der Kommunikation durch das drahtlose LAN, selbst wenn die Bevölkerungsdichte in den Mengen niedrig ist.

[0367] Fig. 56 ist ein erläuterndes Bild eines Kommunikationsverfahrens gemäß der elften Ausführungsform der vorliegenden Erfindung. Bei diesem Kommunikationsverfahren sind Anschlußeinrichtungen **1050a** und **1050b** zum Ermöglichen der Bildung des drahtlosen LAN in dem Bereich eingebaut, in dem die Funkwelle Schwierigkeiten beim Eintreten hat, wie ein unterirdisches Einkaufsgebiet. Die Anschlußeinrichtungen **1050a** und **1050b** sind bevorzugt öffentliche Telefone, die zum Beispiel in den Nähen von Läden in dem unterirdischen Einkaufsgebiet eingebracht sind. In diesem Fall weisen die Anschlußeinrichtungen **1050a** und **1050b** jeweils eine Fernverkehrseinheit **1057** zum Durchführen einer ursprünglichen Funktion des öffentlichen Telefones als auch eine Nahverkehrseinheit **848** auf. Selbst wenn die Bevölkerungsdichte der Menge niedrig ist, können die Anschlußeinrichtungen **850a** und **850b** die Nahverkehrseinheiten **848** der Anschlußeinrichtungen **1050a** und **1050b** als Relais zum Herstellen der Kommunikation durch das drahtlose LAN benutzen.

12. zwölfte Ausführungsform

[0368] Bei der zwölften Ausführungsform wird eine Erörterung über wünschenswertere Beispiele des Halbleiterelementes **401**, der Codierschaltung **402** und der Komperatorschaltung **403** gegeben, die in den obigen Ausführungsformen erörtert wurden.

12.1. Beispiele der Halbleitervorrichtung

[0369] Fig. 57 ist ein Schaltbild, das ein Beispiel des Halbleiterelementes **401** zeigt. Dieses Halbleiterelement **401a** weist eine Mehrzahl von TFTs **101** ($4 \times 4 = 16$ TFTs **101** in dem Beispiel von Fig. 57) auf, die in einer Matrix auf einem Halbleitersubstrat angeordnet sind. Auf dem Halbleitersubstrat ist eine Mehrzahl von Wortleitungen WL1 bis WL4 und eine Mehrzahl von Bitleitungen BL1 bis BL4 weiter in der horizontalen bzw. vertikalen Richtung angeordnet. [0370] Entsprechende Gateelektroden der vier TFTs **101**, die horizontal angeordnet, sind gemeinsam mit jeder der Wortleitungen WL1 bis WL4 verbunden. Andererseits sind entsprechende Drainelektroden der vier TFTs **100**, die verti-

kal angeordnet sind, gemeinsam mit jeder der Bitleitungen BL1 bis BL4 verbunden. Entsprechende Sourceelektroden der 16 TFTs 100 sind gemeinsam mit einer positiven Stromversorgungsleitung verbunden. Weiter ist ein Ende einer jeden der Bitleitungen BL1 bis BL4 mit einer Masseversorgungsleitung durch eine Bitleitungslast 17 verbunden.

[0371] Ein Draht 18 zum Abnehmen des Analogsignals An ist mit einem Ende der Bitleitungslast 17 gegenüber der Masseleitung verbunden. Weiter ist eine Anschlußfläche 15 mit dem anderen Ende einer jeden Bitleitung BL1 bis BL4 verbunden, und eine Anschlußfläche 16 ist mit einem Ende einer jeden der Wortleitungen WL1 bis WL4 verbunden.

[0372] Da das Halbleiterelement 401a den obigen Aufbau aufweist, fließen, wenn eine Gatespannung eines vorbestimmten Pegels an die Wortleitung WL1 bis WL4 angelegt wird, Drainströme Id1 bis Id4 in den vier TFTs 101, die mit der Wortleitung verbunden sind. Da die Drainströme Id1 bis Id4 in die Bitleitungslasten 17 fließen, werden Potentiale proportional zu den Drainströmen Id1 bis Id4 an den Drähten 18 entwickelt, die mit den Bitleitungen BL1 bis BL4 verbunden sind. Die vier Potentiale werden nach außen als die Analogsignale An ausgegeben. Durch sequentielles Anlegen der Gatespannung an die Wortleitungen WL1 bis WL4 können insgesamt 16 Potentiale als die Analogsignale An abgenommen werden.

[0373] Die 16 analogen Signale An werden durch die Codierschaltung 402 codiert, wobei sie in ein 16 Bit Digitalsignal umgewandelt werden, wie zum Beispiel in Fig. 58 gezeigt ist. In Fig. 58 ist der 16 Bit Code in einer Matrix angeordnet, so daß die Beziehung zwischen den TFTs 101, auf denen der Code beruht, und den Bitleitungen BL1 bis BL4 und den Wortleitungen WL1 bis WL4, die damit verbunden sind, verstanden werden kann.

12.2. Beispiel der Codierschaltung und der Komperatorschaltung

[0374] Fig. 59 ist ein Blockschaltbild, das einen Aufbau einer Halbleitervorrichtung zeigt, die das Halbleitersubstrat CH3 (oder CH1) von Fig. 1 benutzt. Diese Halbleitervorrichtung 404a weist das in Fig. 57 gezeigte Halbleiterelement 401a auf. Die Halbleitervorrichtung 404a weist einen Decodiertreiber 410 zum Treiben von jeder der Mehrzahl von Wortleitungen WL1 bis WL4 in dem Halbleiterelement 401a auf der Grundlage eines Adreßsignales Adr auf. Das Adreßsignal Adr kann von außen durch Eingangsanschlüsse eingegeben werden.

[0375] Ein Code Cd, der von der Codierschaltung 402 ausgegeben wird, wird nicht nur an die Komperatorschaltung 403 eingegeben, sondern auch zu der Außenseite durch eine Pufferschaltung 411 ausgegeben. Dieses erlaubt begrenzten Personen, den Identifikationscode Cd zuvor zu kennen. Da die Pufferschaltung 411 vorgesehen ist, ist es möglich, einen Betrug des Eingebens eines Codes unterschiedlich von dem Identifikationscode Cd, der von der Codierschaltung 402 ausgegeben wird, von der Außenseite durch Ausgangsanschlüsse für den Identifikationscode Cd der Komperatorschaltung 403 zu verhindern.

[0376] Da das Halbleiterelement 401a die Anschlußflächen 15 und 16 aufweist, ist es möglich direkt die Analogsignale An auszulesen, in dem ein eine Sonde an die Anschlußflächen 15 und 16 bei dem Herstellungsvorgang der Halbleitervorrichtung 404a angelegt wird. Das ausgelesene Analogsignal An kann in den Identifikationscode Cd umgewandelt werden durch Benutzen einer Einrichtung mit dem gleichen Eigenschaftsmerkmal wie die Codierschaltung 402, und der Identifikationscode Cd kann hier ebenfalls erhalten werden. Wenn daher der Identifikationscode Cd nicht an ei-

nem Platz ausgelesen werden soll, der nicht das Herstellungswerk für die Halbleitervorrichtung 404a ist, können der Eingangsanschluß für das Adreßsignal Adr, die Ausgangsanschlüsse für den Identifikationscodes Cd und die Pufferschaltung 411 entfernt werden.

[0377] Die Komperatorschaltung 403 gibt das Adreßsignal Adr an den Decodiertreiber 410 ein, wenn sie den Speichercode Co, der durch die Eingangsanschlüsse eingegeben wird, mit dem Identifikationscode Cd vergleicht. Da die Halbleitervorrichtung 404a dazu getrieben wird zum Auslesen des Analogsignals An, ist es möglich, den Identifikationscode Cd mit dem Speichercode Co zu vergleichen, ohne daß das Adreßsignal von der Außenseite eingegeben wird.

[0378] Fig. 60 ist ein Schaltbild eines Beispiels der Codierschaltung 402, das einen Schaltabschnitt zeigt, der mit der Bitleitung BL1 verbunden ist. Der gleiche Schaltabschnitt, wie er in Fig. 60 gezeigt ist, ist auch mit den anderen Bitleitungen BL2 bis BL4 verbunden. Die Codierschaltung 402a weist einen Leseverstärker 190 auf. Der Leseverstärker 190 vergleicht das Potential an dem Draht 80 mit einem Referenzpotential Vref, das von Transistoren 192 und 193 erzeugt ist, zum Erzeugen eines Signales eines hohen Pegels oder einen niedrigen Pegels, und er gibt das Signal als 1 Bit des Identifikationscodes Cd aus (z. B. ein Identifikationscode Cd(1) entspricht der Bitleitung BL1).

[0379] In dem Leseverstärker 190 sind eine Reihenschaltung, die aus einem NMOS-Transistor 194 und einem PMOS-Transistor 195 besteht, und eine Reihenschaltung, die aus einem NMOS-Transistor 196 und einem PMOS-Transistor 197 besteht, zwischen die obere Stromversorgungsleitung und die Masseleitung eingefügt. Eine Gateelektrode und eine Drainelektrode des PMOS-Transistors 195 und eine Gateelektrode des PMOS-Transistors 197 sind miteinander verbunden, wodurch eine Stromspiegelschaltung dargestellt wird.

[0380] Der Drainstrom, der in dem TFT 101 fließt, weist einen niedrigen Wert innerhalb eines Bereiches von 1 pA (10^{-12} A) bis ungefähr 1 μ A auf. Daher ist es wünschenswert den Drainstrom auf ungefähr 1 nA (10^{-9} A) zu setzen, in dem ein NMOS-Transistor als die Bitlast 17 benutzt wird und ein konstantes Potential an seine Gateelektrode angelegt wird. Dieses vergrößert die Empfindlichkeit des Leseverstärkers 190. Es ist wünschenswert, ein Gatepotential auf das Massepotential zu setzen, damit der Drainstrom auf ungefähr 1 nA gesetzt wird.

[0381] Eine Reihenschaltung, die aus dem NMOS-Transistor 192 und dem PMOS-Transistor 193 besteht, ist zwischen die Masseleitung und die positive Stromversorgungsleitung eingefügt, und das Referenzpotential Vref wird von Knoten der zwei Transistoren abgenommen. Konstante Potentiale wie das Potential der Masseleitung und das Potential der positiven Stromversorgungsleitung werden an Gateelektroden des NMOS-Transistors 192 bzw. des PMOS-Transistors 193 angelegt. Der Vergleich des Potentials des Drahtes 18 mit dem Referenzpotential Vref ist äquivalent dem Vergleich des Drainstromes des TFT 101 mit einem Referenzstrom Ir (oder seiner Konstantvielfachheit), der durch die Reihenschaltung des NMOS-Transistors 192 und des PMOS-Transistors 193 fließt.

[0382] Zum Sicherstellen des Vergleiches ist es wünschenswert, daß die Transistoren, die nicht der TFT 101 in Fig. 60 ist, Blocktransistoren sein sollten. Wenn die Transistoren, die nicht der TFT 101 sind, polykristalline TFTs sind wie der TFT 101 ist es wünschenswert, daß die Gatelänge und die Gatebreite der Transistoren größer als jene des TFT 101 gesetzt werden, damit die Stabilität der Größe des Drainstromes darin sichergestellt bleibt.

12.3. Anderes Beispiel der Halbleitervorrichtung

[0383] Das Halbleiterelement 401 kann ein polykristallines Widerstandselement oder ein polykristallines Kapazitätselement anstelle des polykristallinen TFT 101 aufweisen. Solch ein Beispiel wird unten erörtert.

[0384] Fig. 61 ist ein Schaltbild, das ein anderes Beispiel des Halbleiterelementes 401 mit einem polykristallinen Widerstandselement zeigt. Dieses Halbleiterelement 401b weist eine Mehrzahl von Widerstandselementen 43 ($4 \times 4 = 16$) Widerstandselemente 43 in dem Beispiel von Fig. 61) auf, die in einer Matrix auf einem Halbleitersubstrat angeordnet sind. Das Widerstandselement 43 weist eine Widerstandssubstanz auf, die aus polykristallinem Halbleiter wie polykristallines Silizium besteht. Daher variiert der Widerstandswert zufällig in dem Widerstandselement 43.

[0385] Auf dem Halbleitersubstrat sind weiter eine Mehrzahl von Wortleitungen WL1 bis WL4 und eine Mehrzahl von Bitleitungen BL1 bis BL4 weiter in der horizontalen bzw. vertikalen Richtung angeordnet.

[0386] Das jeweilige eine Ende der vier Widerstandselemente 43, die horizontal angeordnet sind, sind gemeinsam mit jeder der Wortleitungen WL1 bis WL4 verbunden. Andererseits sind die entsprechenden anderen Enden der vier Widerstandselemente 43, die vertikal angeordnet sind, gemeinsam mit jeder der Bitleitungen BL1 bis BL4 verbunden. Weiter ist ein Ende einer jeden der Bitleitungen BL1 bis BL4 mit der Masseleitung durch einen NMOS-Transistor 48 als eine Bitleitungslast verbunden.

[0387] Ein Draht 49 zum Herausführen des Analogsignales An ist mit einer Drainelektrode des NMOS-Transistors 48 verbunden. Weiter ist die Anschlußfläche 15 mit dem anderen Ende einer jeden der Bitleitungen BL1 bis BL4 verbunden, und die Anschlußfläche 16 ist mit einem Ende einer jeden Wortleitung WL1 bis WL4 verbunden.

[0388] Da das Halbleiterelement 401b den obigen Aufbau aufweist, fließen, wenn eine Gatespannung eines vorbestimmten Pegels an eine der Wortleitungen WL1 bis WL4 angelegt wird, Ströme in den vier Widerstandselementen 43, die mit der Wortleitung verbunden sind. Da die Ströme in den NMOS-Transistor 48 fließen, entwickeln sich Potentiale proportional zu den Strömen, die durch die Widerstandselemente 43 fließen, an den Drähten 49, die mit den Bitleitungen BL1 bis BL4 verbunden sind. Die vier Potentiale werden nach außen als die Analogsignale An ausgegeben. Durch sequentielles Anlegen der vorbestimmten Potentiale an die Wortleitungen WL1 bis WL4 können insgesamt 16 Potentiale als die Analogsignale An abgenommen werden. Die Analogsignale An können als Zufallswerte entsprechend den variierenden Widerständen der Widerstandselemente 43 erhalten werden.

[0389] Da das Halbleiterelement 401b die Anschlußflächen 15 und 16 aufweist, ist es möglich die Analogsignale An unter Benutzung einer Sonde bei dem Herstellungsvorgang des Halbleiterelementes 401b zu lesen. Weiterhin kann es einen anderen Fall geben, in dem die Widerstandselemente 43 in einer linearen Matrix angeordnet sind und jeweils ein Ende aller Widerstandselemente 43 mit einer einzelnen Wortleitung verbunden sind. Zum Erhöhen der Variation der Analogsignale An werden die Länge und die Breite der polykristallinen Substanz des Widerstandselementes 43 bevorzugt in den gleichen Bereich wie die optimale Bedingung für die Gatelänge L und die Gatebreite W gesetzt.

12.4. Noch anderes Beispiel der Halbleitervorrichtung

[0390] Fig. 62 ist ein Schaltbild, das ein noch anderes Beispiel des Halbleiterelementes 401 mit einem kapazitiven

Element aus polykristalliner Substanz zeigt. Dieses Halbleiterelement 401c weist Reihenschaltungen auf, die aus einer Mehrzahl von kapazitiven Elementen 91 ($4 \times 4 = 16$ kapazitiven Elemente 91 in dem Beispiel von Fig. 62) und MOS-Transistoren 90, die in einer Matrix auf einem Halbleitersubstrat angeordnet sind, bestehen. Das kapazitive Element 91 weist eine polykristalline dielektrische Substanz, z. B. eine polykristalline dielektrische Perovskit-Substanz wie BST ($\text{Ba}_x\text{Sr}_{1-x}\text{TiO}_3$) auf. Daher variiert der Kapazitätswert zufällig in dem kapazitiven Element 91.

[0391] Auf dem Halbleitersubstrat sind eine Mehrzahl von Wortleitungen WL1 bis WL4 und eine Mehrzahl von Bitleitungen BL1 bis BL4 weiter in der horizontalen bzw. vertikalen Richtung angeordnet. Entsprechende Gateelektroden der MOS-Transistoren 90, die in den vier Reihenschaltungen enthalten sind, die horizontal angeordnet sind, sind gemeinsam mit jeder der Wortleitungen WL1 bis WL4 verbunden. Andererseits sind entsprechende der Sourceelektroden und der Drainelektroden der MOS-Transistoren 90, die in den vier Reihenschaltungen enthalten sind, die vertikal angeordnet sind, gemeinsam mit jeder der Bitleitungen BL1 bis BL4 verbunden. Entsprechende andere Enden der kapazitiven Elemente 91, die in den 16 Reihenschaltungen enthalten sind, sind mit der Masseleitung verbunden. Die Anschlußfläche 15 ist mit dem anderen Ende einer jeden der Bitleitungen BL1 bis BL4 verbunden, und die Anschlußfläche 16 ist mit dem einen Ende einer jeden der Wortleitungen WL1 bis WL4 verbunden.

[0392] Da das Halbleiterelement 401c den obigen Aufbau aufweist, werden, wenn eine Gatespannung eines vorbestimmten Pegels an eine der Wortleitungen WL1 bis WL4 angelegt wird, die vier MOS-Transistoren, die mit der Wortleitung verbunden sind, eingeschaltet. Durch die MOS-Transistoren, die eingeschaltet sind, werden die anderen Enden der vier kapazitiven Elemente 91 elektrisch mit den Bitleitungen BL1 bis BL4 verbunden. Zu dieser Zeit ist es möglich durch die Bitleitungen BL1 bis BL4, die Kapazitäten der vier kapazitiven Elemente 91 zu messen. Zum Beispiel kann das Potential zu der Zeit, wenn der Strom während einer gegebenen Zeitdauer geliefert wird, gemessen werden und das Potential kann als das Analogsignal An abgenommen werden. Das Potential reflektiert die Kapazität des kapazitiven Elementes 91.

[0393] Durch sequentielles Anlegen der vorbestimmten Gatespannungen an die Wortleitungen WL1 bis WL4 können insgesamt 16 Potentiale als die Analogsignale abgenommen werden. Die Analogsignale An können als Zufallswerte entsprechend den variierenden Kapazitäten der kapazitiven Elemente 91 erhalten werden. Da das Halbleiterelement 401c die Anschlußflächen 15 und 16 aufweist, ist es möglich, die Analogsignale An auszulesen unter Benutzung einer Sonde bei dem Herstellungsvorgang des Halbleiterelementes 401c. Weiter kann es einen anderen Fall geben, in dem die Reihenschaltungen, die jeweils aus den kapazitiven Element 91 und dem MOS-Transistor 90 bestehen, in einer linearen Matrix angeordnet sind, und die Gateelektroden alle MOS-Transistoren 90 sind mit einer einzigen Wortleitung verbunden.

[0394] Zum Erhöhen der Variation der Analogsignal An werden die Länge und die Breite der polykristallinen dielektrischen Substanz der kapazitiven Elemente 91 bevorzugt in den gleichen Bereich wie die optimale Bedingung der Gatelänge L und der Gatebreite W gesetzt. Bei dem BST ist, wenn die Filmdicke 100 nm beträgt, die Filmdicke in Begriffen eines Siliziumoxidfilms ungefähr 0,5 nm. Wenn daher die Form des BST, das der Elektrode zugewandt ist, quadratisch ist mit Seiten von 0,3 μm , beträgt die Kapazität ungefähr 6,2 fF. In einem optimalen Fall, in dem der Durch-

messer eines Kornos (Mittelwert) auf 100 nm gesetzt ist, was der Filmdicke entspricht, variiert die Kapazität in einem Bereich von -30% bis +30%, d. h. in einem Bereich von 4,3 fF bis 8,1 fF. Der Bereich ist ausreichend groß um ihn als Identifikation benutzen zu können.

12.5. Anderes Beispiel der Komperatorschaltung

[0395] Fig. 63 ist ein Blockschaltbild, das einen anderen Aufbau der Halbleitervorrichtung zeigt, die das Halbleiter-substrat CH3 (oder CH1) benutzt. Diese Halbleitervorrichtung 404d weist eine Komperatorschaltung 403a auf, die nicht nur vollständige Übereinstimmung zwischen dem Identifikationscode Cd und dem Speichercode Co, sondern auch eine Annäherung in einem vorbestimmten Bereich beurteilen kann. Ein Referenzwert SL, der für die Beurteilung benutzt wird, kann von der Außenseite des Halbleiterelementes 404d durch einen Eingangsanschluß eingegeben werden.

[0396] Um dieses zu ermöglichen, weist die Komperatorschaltung 403a eine Ablenkschaltung 200 zum Ablenken des Potentials einer Wortleitung WL auf. Der Identifikationscode Cd, der durch Ablenken des Potentials der Wortleitung WL variiert wird, wird durch eine Näherungsberechnungsschaltung 199 mit einigen entsprechenden der Speichercode Co verglichen, die in einem Eingangscodespeicher 198 gespeichert sind. Die Näherungsberechnungsschaltung 199 überträgt einen Grad der Annäherung VA zwischen den Codes, die durch den Vergleich berechnet sind, an eine Entwicklungsschaltung 210. Die Entwicklungsschaltung 210 vergleicht den Grad der Annäherung VA mit dem Referenzwert SL zum Beurteilen, ob der Grad der Annäherung VA nicht weniger als ein gegebener Wert ist oder nicht und gibt das Beurteilungsergebnis als Beurteilungssignal VB aus.

[0397] Das Beurteilungssignal VB wird für jede Wortleitung WL erhalten, die der Decodiertreiber 410 treibt. Eine Adreßerzeugungsschaltung 441 überträgt das Adreßsignal sequentiell, das all die Wortleitungen spezifiziert, eines nach dem andern zu dem Decodiertreiber 410. Während dieser Tätigkeit wird eine Mehrzahl von Beurteilungssignalen VB entsprechend all den Wortleitungen WL sequentiell eines nach dem anderen erhalten.

[0398] Eine Gesamtbeurteilungsschaltung 220 beurteilt die Annäherung zwischen dem Code Cd aller Bits entsprechend aller Wortleitungen und des Codes Co aller Bits auf der Grundlage der Mehrzahl von Beurteilungssignalen VB entsprechend aller Wortleitungen WL und gibt das Freigabesignal En aus, das das Beurteilungsergebnis darstellt. Es ist auch möglich, die Beurteilung der vollständigen Übereinstimmung auszuwählen, die die strikteste Beurteilung der Annäherung ist, durch geeignetes Einstellen des Referenzwertes SL. Wenn es eine Wortleitung gibt, wird die Gesamtbeurteilungsschaltung 220 nicht gebraucht, und das Beurteilungssignal VB wird als das Freigabesignal En ausgegeben.

[0399] Als Reaktion auf ein Befehlssignal St, das durch den Eingangsanschluß eingegeben wird, startet eine Steuerungsschaltung 442 den Betrieb der Elemente in der Komperatorschaltung 403a und steuert den Betrieb der Elemente gemäß einer vorbestimmten Prozedur. Insbesondere wird ein Ablenkschaltssignal SS, das ein Steuersignal ist, das befiehlt, ob das Ablenken durchgeführt werden soll oder nicht, von der Steuerungsschaltung 442 zu der Ablenkschaltung 200 übertragen. Die Annäherungsberechnungsschaltung 199, die Auswertungsschaltung 210 und die Gesamtbeurteilungsschaltung 220 stellen eine Beurteilungsschaltung 440 dar.

1. Halbleitervorrichtung mit:

N Codeerzeugereinheiten (400), wobei $N \geq 1$ ist, die in N Halbleitersubstraten (CH1, CH3-CH6, CH10-CH13, CH20, CH22, CH23, CH40, CH42, CH50, CH52, CH70, CH90, CH91, CH100, CH102, CH103, CH104) in einer Eins-zu-Eins-Entsprechung gebildet sind, wobei jede der N Codeerzeugereinheiten (400) zum Erzeugen eines Identifikationscodes (Cd, Cd1, Cd2) aufgebaut ist, der einem entsprechenden Halbleitersubstrat (CH1, CH3-CH6, CH10-CH13, CH20, CH22, CH23, CH24, CH42, CH50, CH52, CH70, CH90, CH91, CH100, CH102, CH103, CH104) innewohnt; und

N Speicher (601, 654), die in einer Eins-zu-Eins-Entsprechung zu den N Identifikationscodes (Cd, Cd1, Cd2) gebildet sind, wobei jeder der N Speicher (601, 654) einen Code, der mit einem entsprechenden Identifikationscode übereinstimmt, als einen Speichercode (Co, Co1, Co2) speichert,

und jeder der N Speicher (601, 654) in einem anderen Halbleitersubstrat (CH2, CH4-CH6, CH11, CH13, CH20-CH23, CH41, CH51, CH71, CH92, CH103) als ein entsprechendes Halbleitersubstrat (CH1, CH3-CH6, CH10-CH13, CH20, CH22, CH23, CH40, CH42, CH50, CH52, CH70, CH90, CH91, CH100, CH102, CH103, CH104) gebildet ist.

2. Halbleitervorrichtung nach Anspruch 1, bei der jeder der N Speicher (601, 654) einen OTPROM (602) aufweist, der den Speichercode (Co, Co1, Co2) speichert.

3. Halbleitervorrichtung nach Anspruch 1 oder 2, bei der jede der N Codeerzeugereinheiten (400) aufweist: ein Halbleiterelement (401) und

eine Codierschaltung (402), die zum Umwandeln einer elektrischen Eigenschaft des Halbleiterelementes (401) in ein digitales Signal aufgebaut ist, so daß ein Wert des digitalen Signales mit der Variation der elektrischen Eigenschaft des Halbleiterelementes (401) variiert, zum Erzeugen des Identifikationscodes (Cd, Cd1, Cd2) und Ausgeben des Identifikationscodes (Cd, Cd1, Cd2).

4. Halbleitervorrichtung nach Anspruch 3, bei der das Halbleiterelement (401) eine polykristalline Substanz (1060) aufweist und die Variation in der elektrischen Eigenschaft des Halbleiterelementes (401) verursacht wird durch die Variation in der Kristallstruktur der polykristallinen Substanz (1060).

5. Halbleitervorrichtung nach Anspruch 1 oder 2, bei der jede der N Codeerzeugereinheiten (400) einen OTPROM (602) aufweist, der den Identifikationscode (Cd, Cd1, Cd2) speichert.

6. Halbleitervorrichtung nach einem der Ansprüche 1 bis 5, mit:

N Komperatorschaltungen (403), die in einer Eins-zu-Eins-Beziehung zu den N Identifizierungscodes (Cd, Cd1, Cd2) gebildet sind, wobei jede der N Komperatorschaltungen (403) so aufgebaut ist, daß sie einen entsprechenden Identifikationscode (Cd, Cd1, Cd2) und einen entsprechenden Speichercode (Co, Co1, Co2) vergleicht, wodurch beurteilt wird, ob diese Codes miteinander übereinstimmen oder nicht, und ein Freigabesignal (En, En1, En2) ausgibt, das das Beurteilungsergebnis darstellt.

7. Halbleitervorrichtung nach Anspruch 6, bei der jede der N Komperatorschaltungen (403) in dem Halbleitersubstrat (CH1, CH3-CH6, CH11-CH13, CH20, CH22, CH23, CH40, CH42, CH100, CH102, CH103) gebildet

ist entsprechend einem zu vergleichenden entsprechenden Identifikationscode (Cd, Cd1, Cd2).

8. Halbleitervorrichtung nach Anspruch 7, mit:

N Schlüsselerzeugereinheiten (633), N Verschlüsselungsschaltungen (631) und N Decodierschaltungen (632), die in einer Eins-zu-Eins-Entsprechung zu den N Identifikationscodes (Cd, Cd1, Cd2) gebildet sind, wobei jede der N Schlüsselerzeugereinheiten (633), jede der N Verschlüsselungsschaltungen (631) und jede der N Decodierschaltungen (632) in dem Halbleitersubstrat (CH20, CH22, CH23, CH40, CH42) entsprechend einem entsprechenden Identifikationscode (Cd, Cd1, Cd2) gebildet ist, worin jede der N Schlüsselerzeugereinheiten (633) einen Schlüssel (K, K1, K2) zur Verschlüsselung einem entsprechenden Halbleitersubstrat (CH20, CH22, CH23, CH40, CH42) innewohnend erzeugt, jede der N Verschlüsselungsschaltungen (631) den Identifikationscode (Cd, Cd1, Cd2), der von der Codeerzeugereinheit (400) erzeugt ist, die in einem entsprechenden Halbleitersubstrat (CH20, CH22, CH23, CH40, CH42) gebildet ist, auf der Grundlage eines entsprechenden Schlüssels (K, K1, K2) und den Identifikationscode (Cd#, Cd1#, Cd2#) der verschlüsselten Form zu dem entsprechenden Speicher (601) überträgt, jeder der N Speicher (601) den Identifikationscode (Cd#, Cd1#, Cd2#) der verschlüsselten Form, der von einer entsprechenden Verschlüsselungsschaltung (631) ausgegeben ist, als der Speichercode (Co#, Co1#, Co2#) der verschlüsselten Form speichert, jede der N Decodierschaltungen (632) den Speichercode (Co#, Co1#, Co2#) der verschlüsselten Form, der in dem entsprechenden Speicher (601) gespeichert ist, auf der Grundlage eines entsprechenden Schlüssels (K, K1, K2) decodiert und jede der N Komparator-schaltungen (403) den Identifikationscode (Cd, Cd1, Cd2), der von einer entsprechenden Erzeugereinheit (400) erzeugt ist, mit dem Speichercode (Co, Co1, Co2), der von einer entsprechenden Decodierschaltung (632) decodiert ist, vergleicht.

9. Halbleitervorrichtung nach Anspruch 8, bei der jede der N Schlüsselerzeugereinheiten (633) ein anderes Halbleiterelement (401), eine andere Codierschaltung (402) zum Umwandeln einer elektrischen Eigenschaft des anderen Halbleiterelementes (401) in ein anderes Digitalsignal aufweist, so daß ein Wert des anderen Digitalsignales mit der Variation der elektrischen Eigenschaft des anderen Halbleiterelementes (401) variiert zum Erzeugen des Schlüssels (K, K1, K2) und Ausgeben des Schlüssels.

10. Halbleitervorrichtung nach Anspruch 9, bei der das andere Halbleiterelement (401) eine andere polykristalline Substanz (1060) aufweist und die Variation in der elektrischen Eigenschaft des anderen Halbleiterelementes (401) durch die Variation in der Kristallstruktur der anderen polykristallinen Substanz (1060) verursacht wird.

11. Halbleitervorrichtung nach Anspruch 8, bei der jede der N Schlüsselerzeugereinheiten (633) einen OTPROM (602) aufweist, der den Schlüssel (K, K1, K2) speichert.

12. Halbleitervorrichtung nach einem der Ansprüche 7 bis 11, mit:

N Umschalt-schaltungen (641), die in einer Eins-zu-Eins-Entsprechung mit den N Identifikationscodes gebildet sind, wobei jede der N Umschalt-schaltungen in dem Halbleitersubstrat (CH40, CH42) entsprechend ei-

nem entsprechenden Identifikationscode (Cd, Cd1, Cd2) gebildet ist, jede der N Umschalt-schaltungen (641) so aufgebaut ist, daß sie exklusiv eine Übertragung eines entsprechenden Identifikationscodes (Cd, Cd1, Cd2), der von einer entsprechenden Codeerzeugereinheit (400) erzeugt ist, zu einem entsprechenden Speicher (601) und eine Eingabe des Speicher-codes (Co, Co1, Co2), der in dem entsprechenden Speicher (601) gespeichert ist, zu einer entsprechenden Komparator-schaltung (403) durchführt.

13. Halbleitervorrichtung nach einem der Ansprüche 6 bis 12, mit:

einer vorbestimmten Schaltung (405), die einen Schaltungsabschnitt (460) enthält, der selektiv in einen aktiven Zustand oder in einen inaktiven Zustand kommt in Abhängigkeit der N Freigabesignale (En, En1, En2) entsprechend den N Identifikationscodes (Cd, Cd1, Cd2).

14. Halbleitervorrichtung nach Anspruch 13, worin die vorbestimmte Schaltung (405) in einem (CH1, CH4, CH10, CH20, CH40, CH50, CH70, CH90, CH100, CH103) der N Halbleitersubstrate (CH1, CH3-CH6, CH10-CH13, CH20, CH22, CH23, CH40, CH42, CH50, CH52, CH70, CH90, CH91, CH100, CH102, CH103, CH104) zusammen mit einer entsprechenden Komparator-schaltung (403) gebildet ist.

15. Halbleitervorrichtung nach einem der Ansprüche 1 bis 14, bei der die Zahl N = 1 ist.

16. Halbleitervorrichtung nach einem der Ansprüche 1 bis 14, bei der die Zahl N = 2 ist und jede der N Codeerzeugereinheiten (400) und ein entsprechender Speicher (601) entsprechend in dem einen und dem anderen der N Halbleitersubstrate (CH4-CH6, CH10, CH11, CH13, CH20, CH22, CH23, CH103) gebildet sind.

17. Anschlußeinrichtung mit: der Halbleitervorrichtung (1002, 1012), wie sie in Anspruch 13 oder 14 definiert ist, worin die vorbestimmte Schaltung (405) eine Kommunikationsschaltung (405a) zum Übertragen und Empfangen eines Signales zu der Außenseite und von der Außenseite ist und

mindestens eines des Übertragens und des Empfangens gestoppt wird, wenn die N Freigabesignale (En, En1, En2) Nichtübereinstimmung von mindestens einem der N Identifikationscodes (Cd, Cd1, Cd2) und eines entsprechenden Speicher-codes (Co, Co1, Co2) anzeigen.

18. Anschlußeinrichtung mit: der Halbleitereinrichtung (1002, 1012), wie sie in einem der Ansprüche 6 bis 12 definiert ist; und einer Kommunikationsschaltung (405a), die zum Übertragen und Empfangen eines Signales an die Außenseite und von der Außenseite aufgebaut ist, worin die Kommunikationsschaltung (405a) die N Freigabesignale (En, En1, En2) als Teil des Signales zu der Außenseite überträgt.

19. Anschlußeinrichtung mit: der Halbleitervorrichtung (652, 801, 811), wie sie in einem der Ansprüche 1 bis 5 definiert ist; und einer Kommunikationsschaltung (405a), die zum Übertragen und Empfangen eines Signales an die Außenseite und von der Außenseite aufgebaut ist, worin die Kommunikationsschaltung (405a) die N Identifikationscodes (Cd, Cd1, Cd2) und die N Speicher-codes (Co, Co1, Co2) als Teil des Signales zu der Außenseite überträgt.

20. Anschlußeinrichtung nach Anspruch 19, worin die Zahl N = 1 ist,

die N Codeerzeugereinheiten (400) und die Kommuni-

kationsschaltung (405) in einem Hauptkörperabschnitt (651, 671, 691) enthalten sind und die N Speicher (654) in einem Hilfsabschnitt (653) enthalten ist, der von dem Hauptkörperabschnitt (651, 671, 691) abnehmbar ist.

5

Hierzu 52 Seite(n) Zeichnungen

10

15

20

25

30

35

40

45

50

55

60

65

FIG. 1

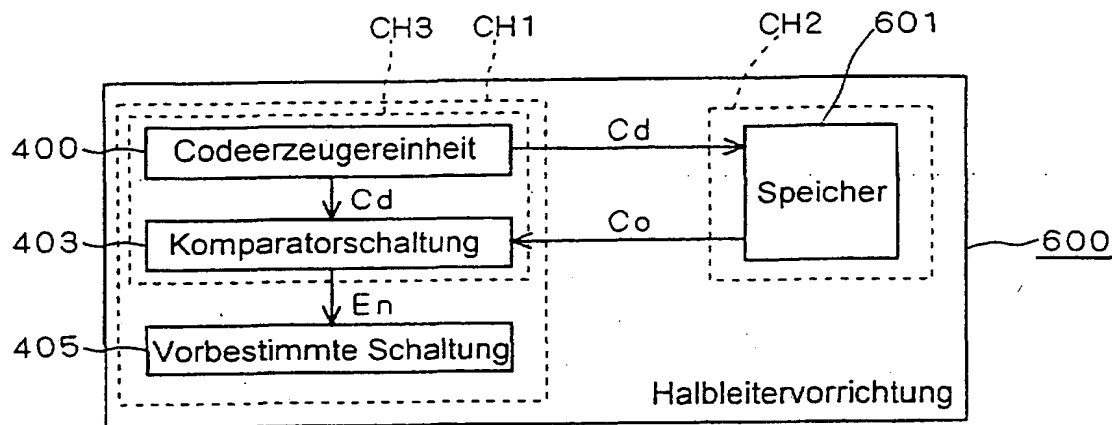


FIG. 2

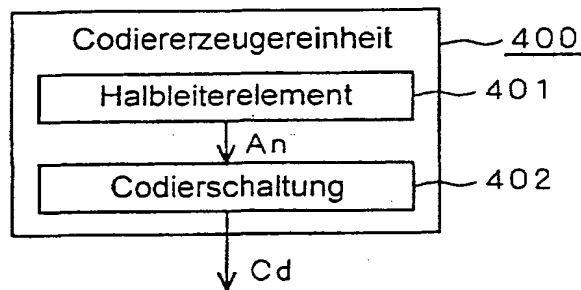


FIG. 3

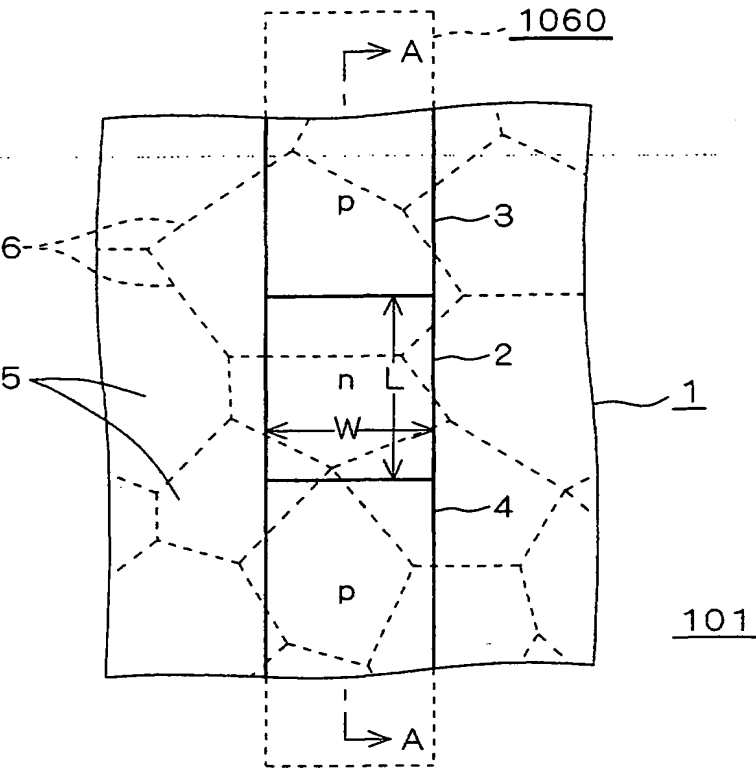


FIG. 4

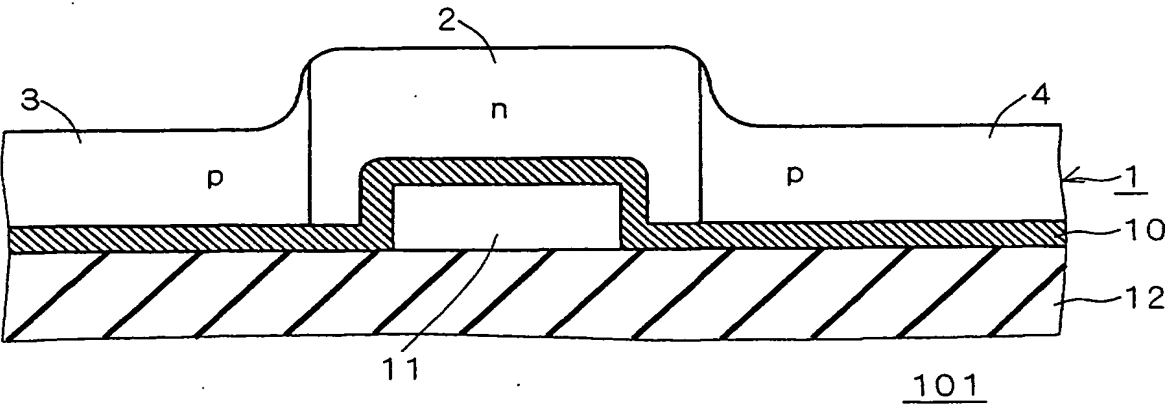


FIG. 5

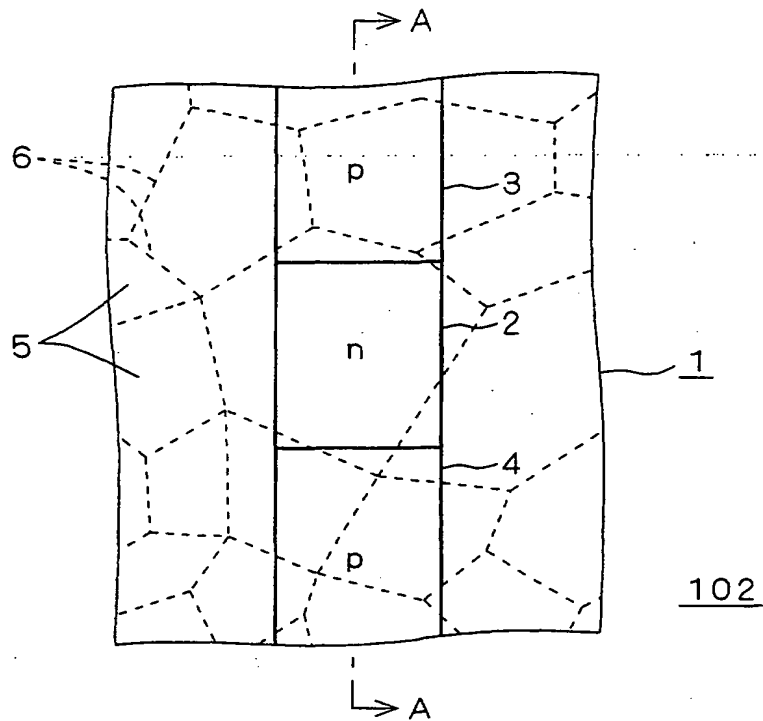


FIG. 6

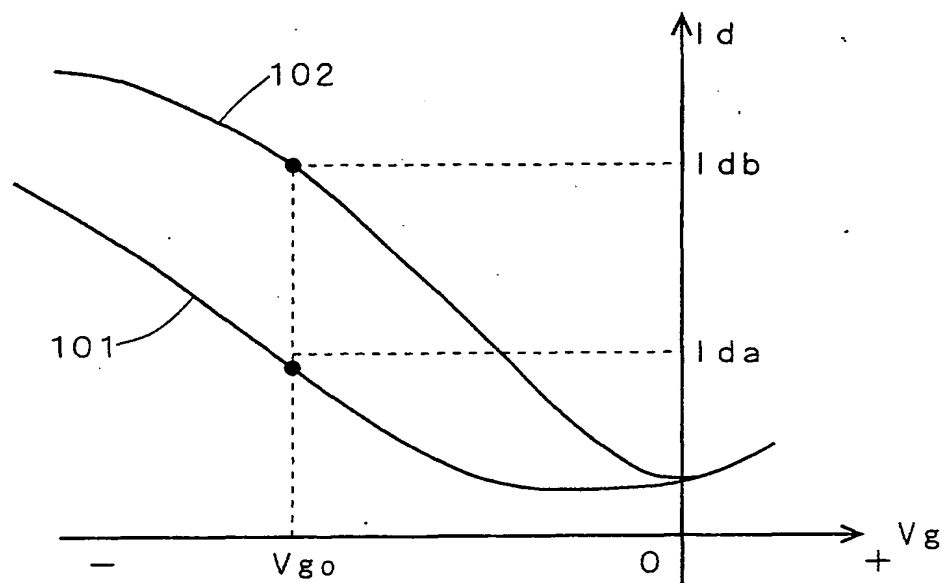


FIG. 7

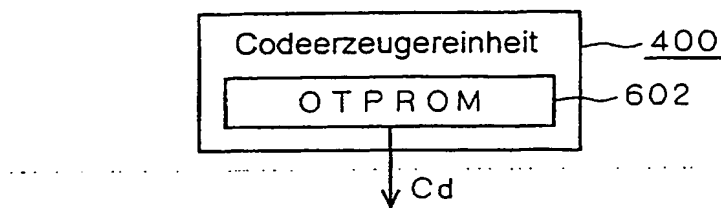


FIG. 8

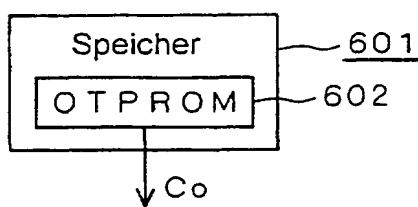


FIG. 9

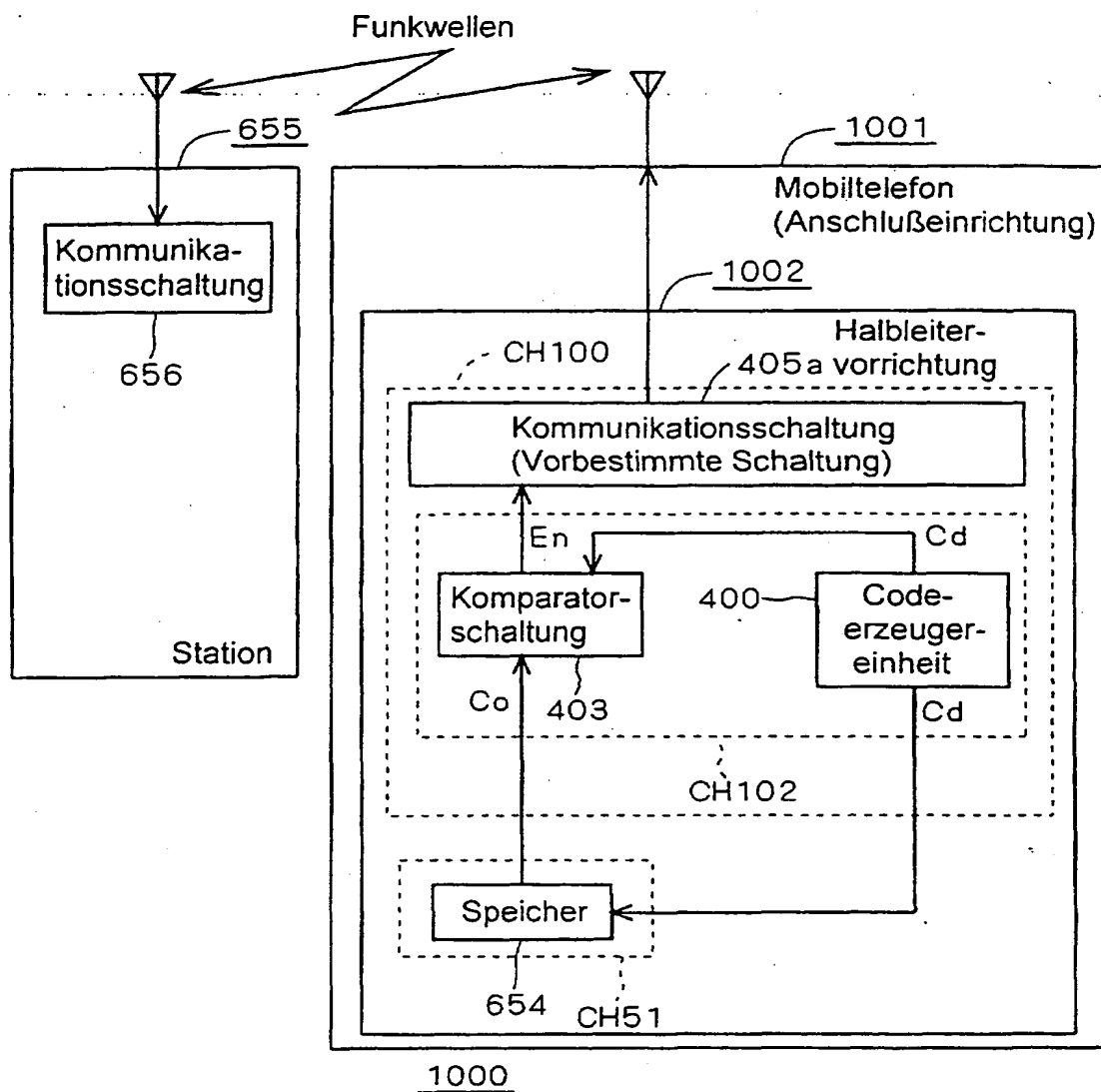


FIG. 10

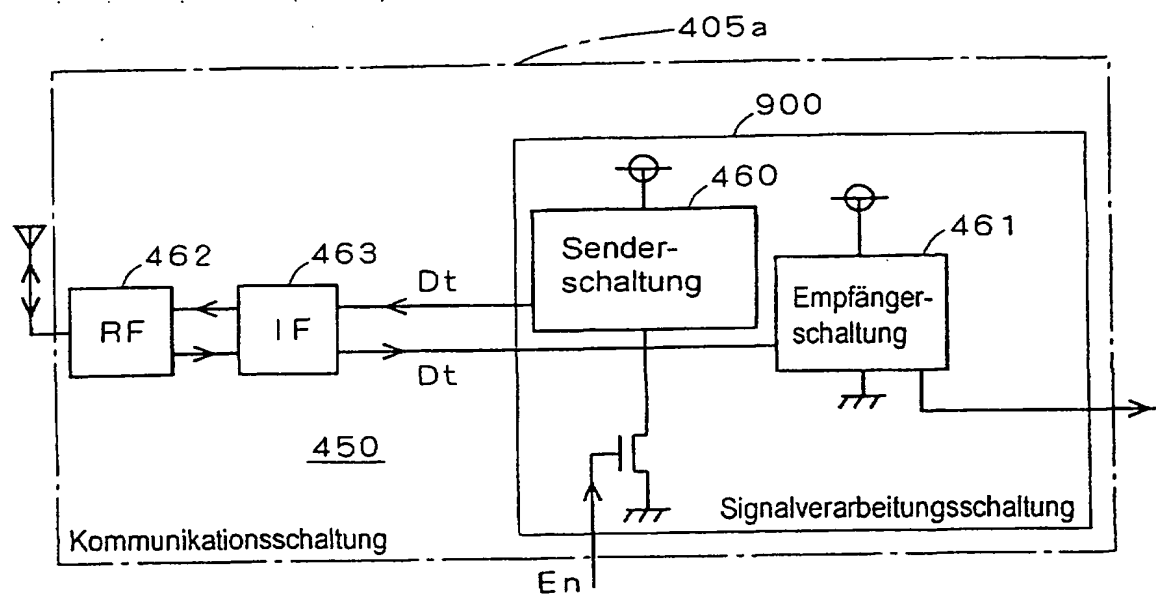


FIG. 11

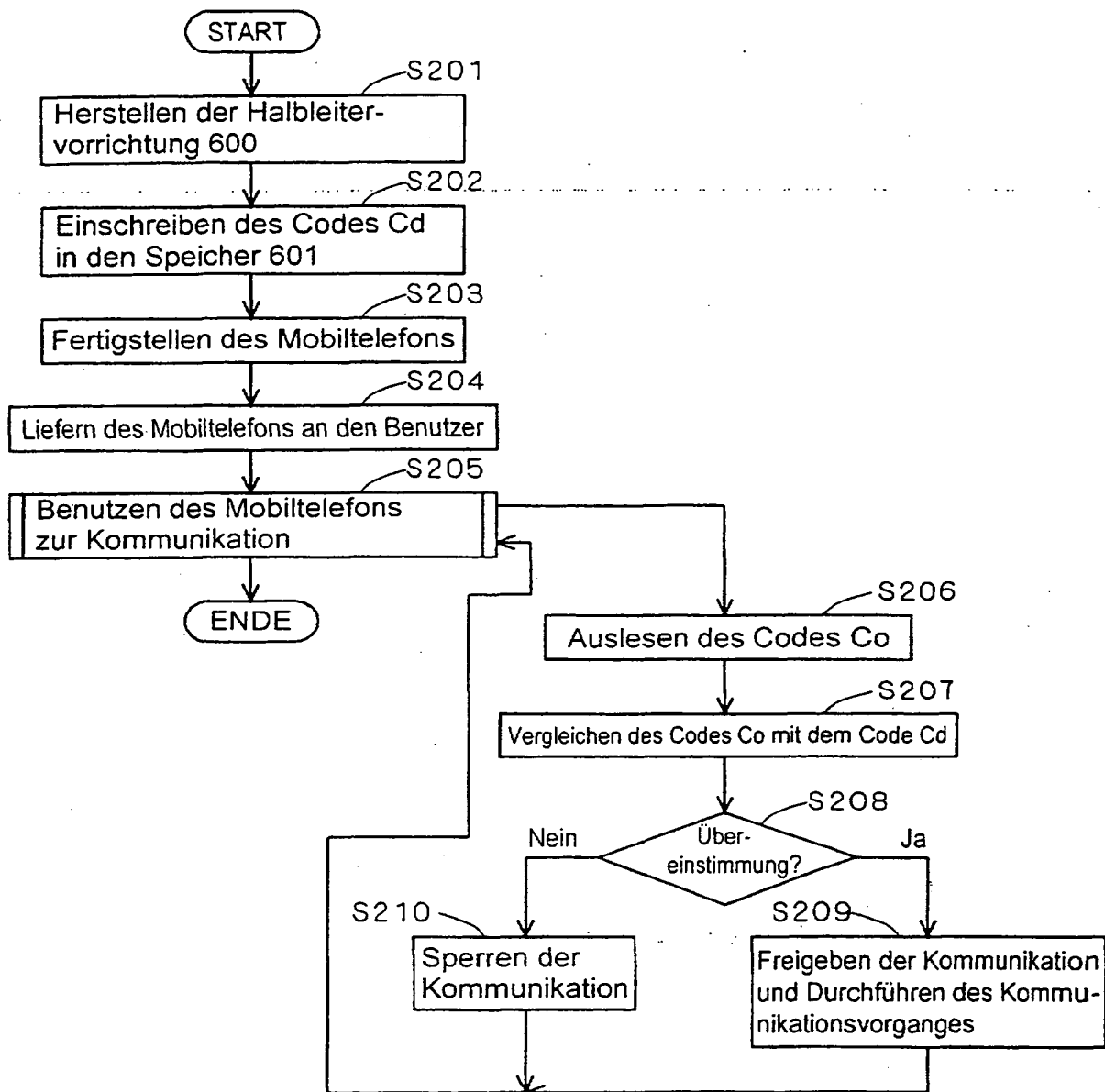


FIG. 12

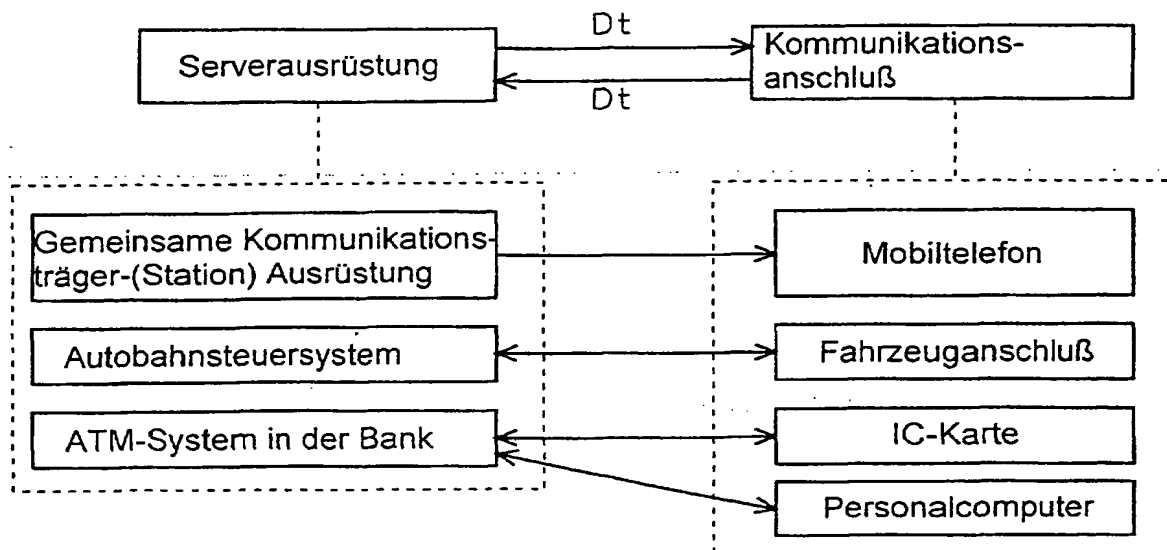


FIG. 13

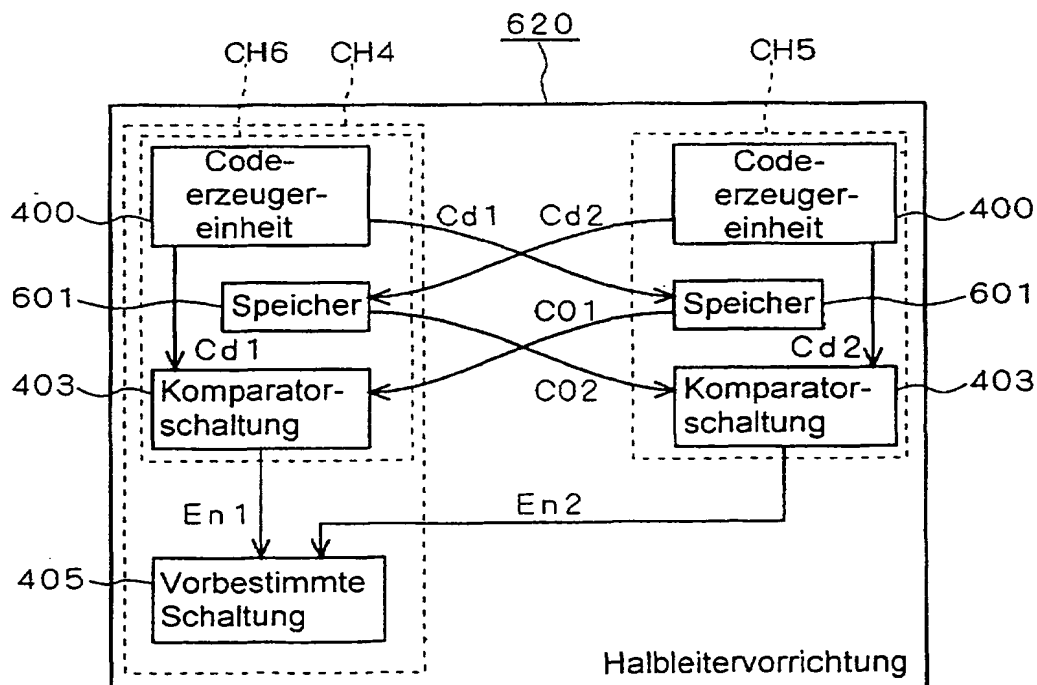


FIG. 14

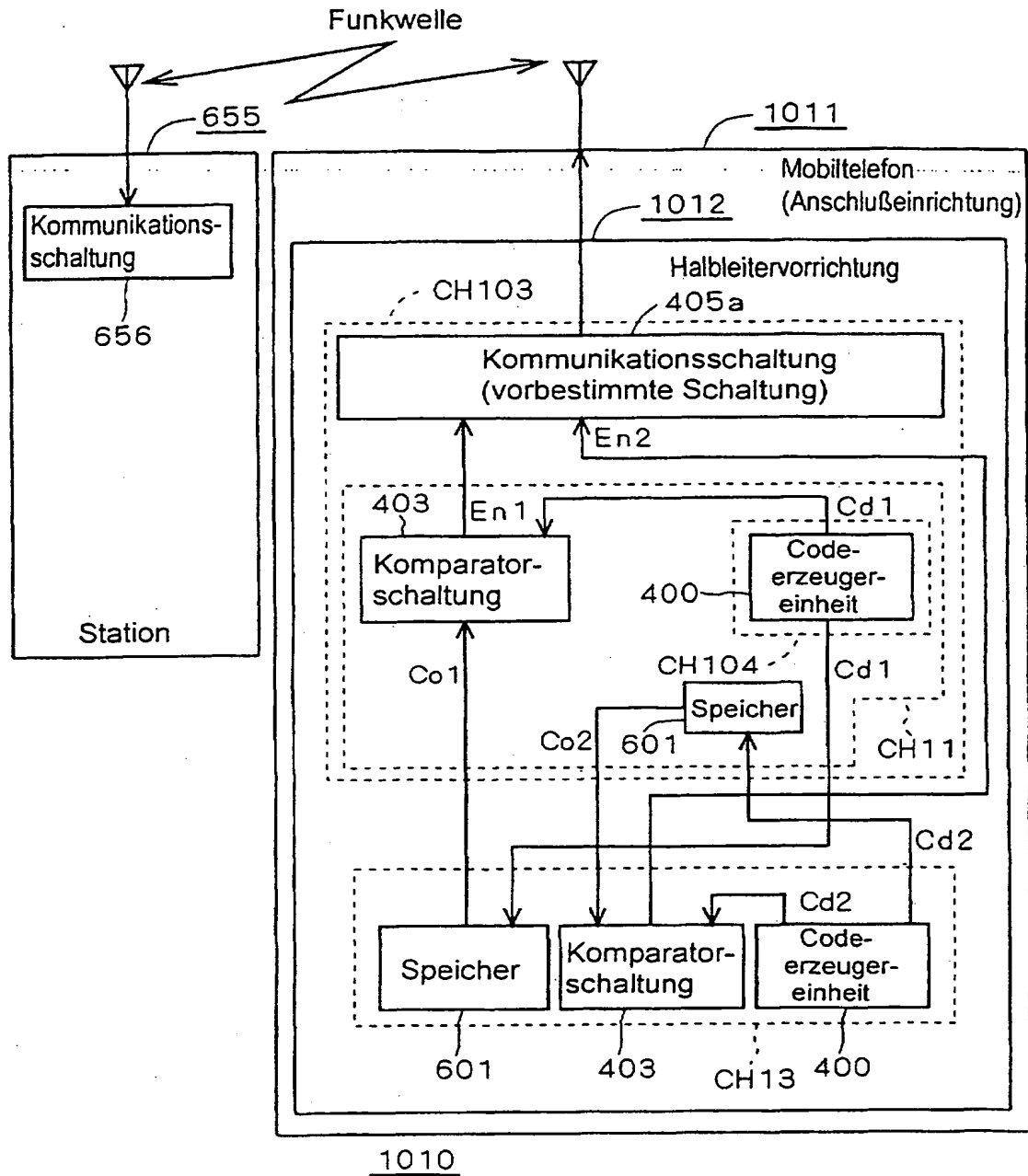


FIG. 15

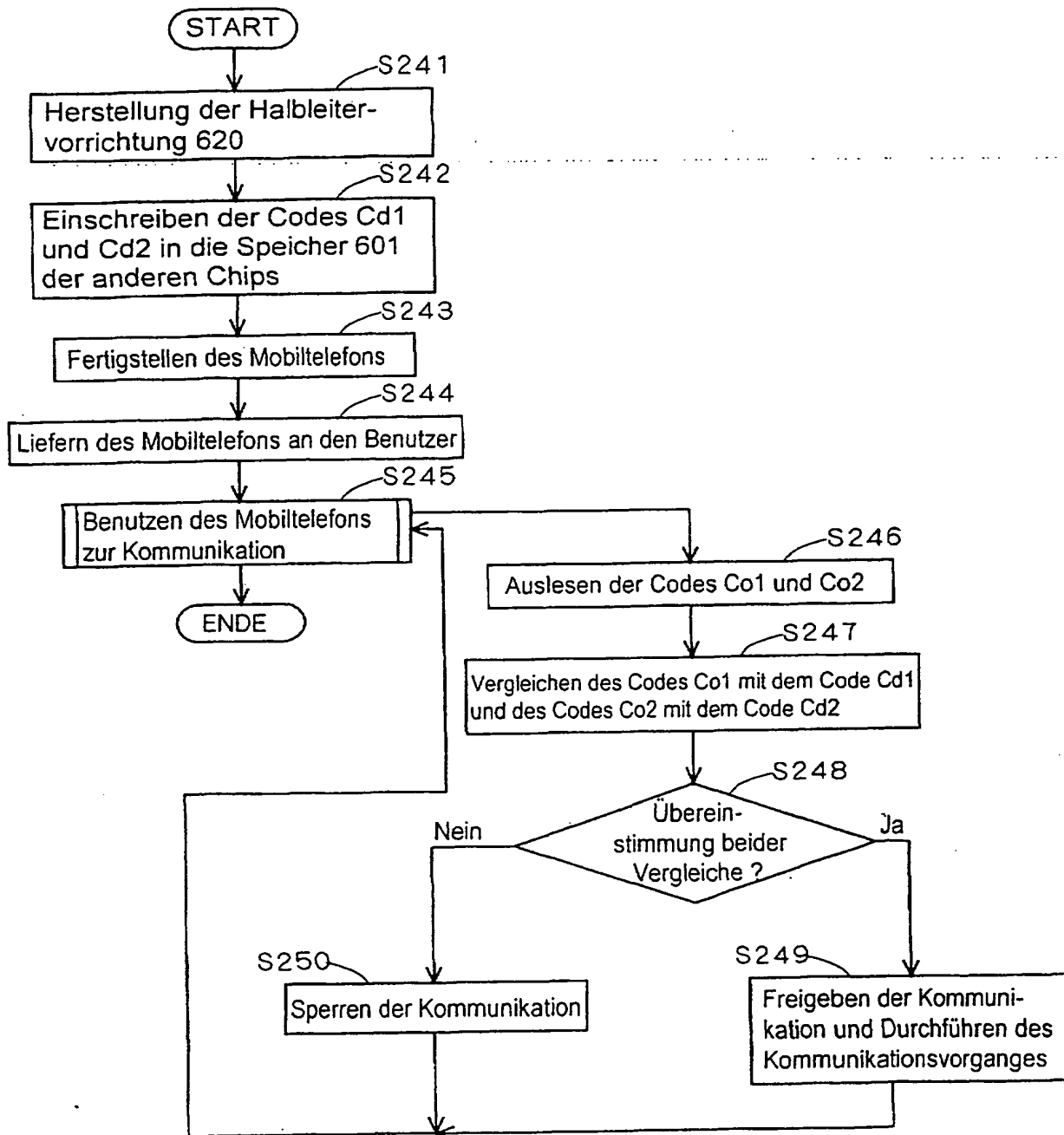


FIG. 16

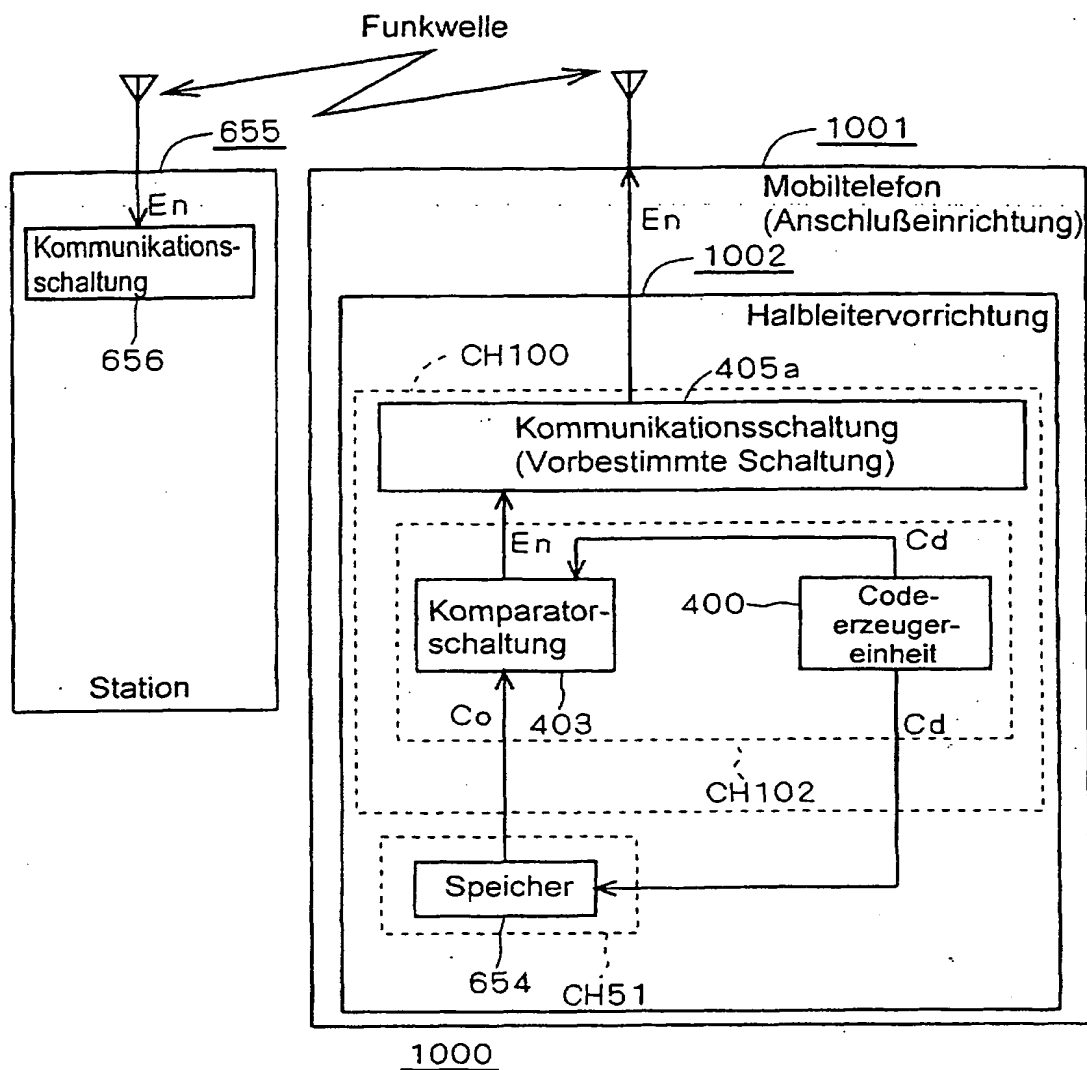


FIG. 17

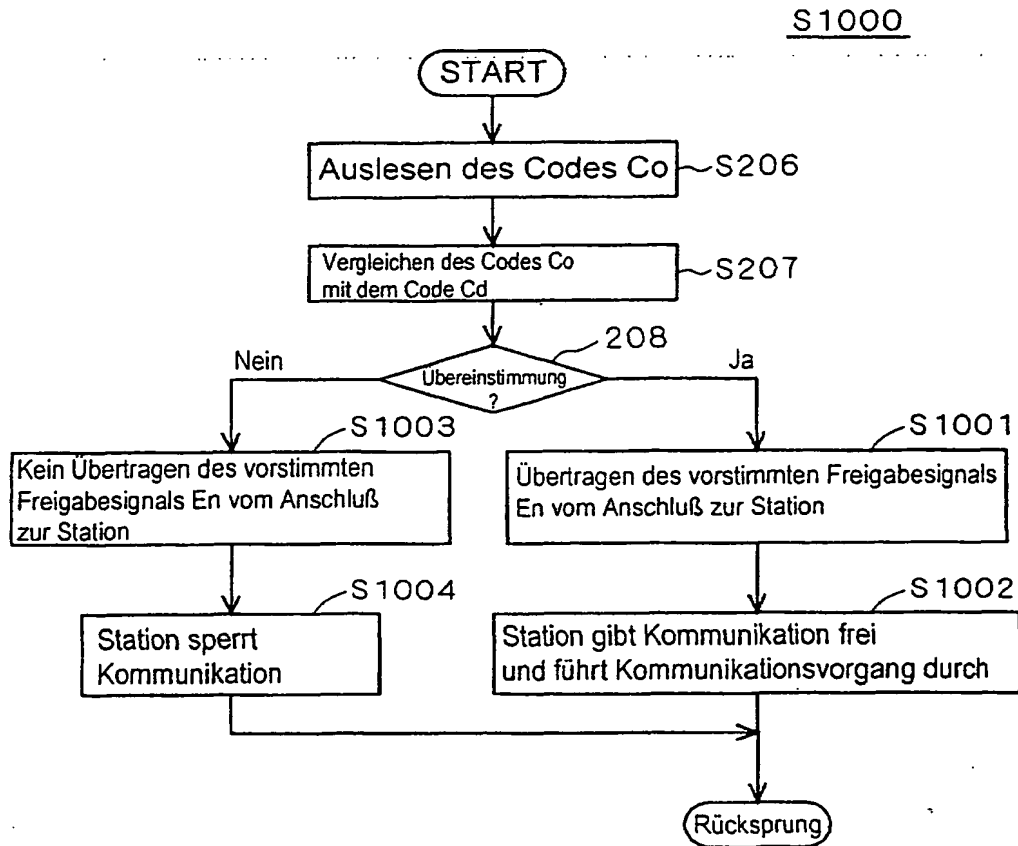


FIG. 19

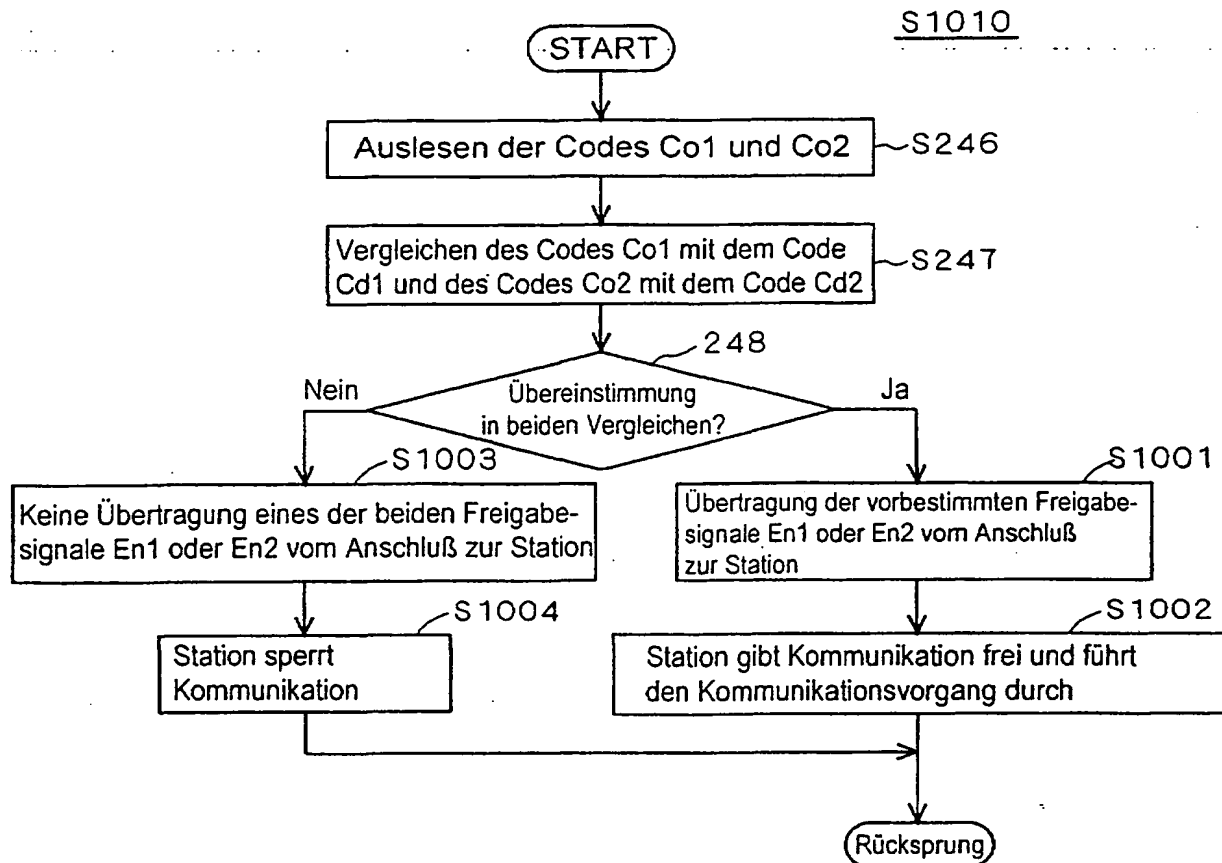


FIG. 20

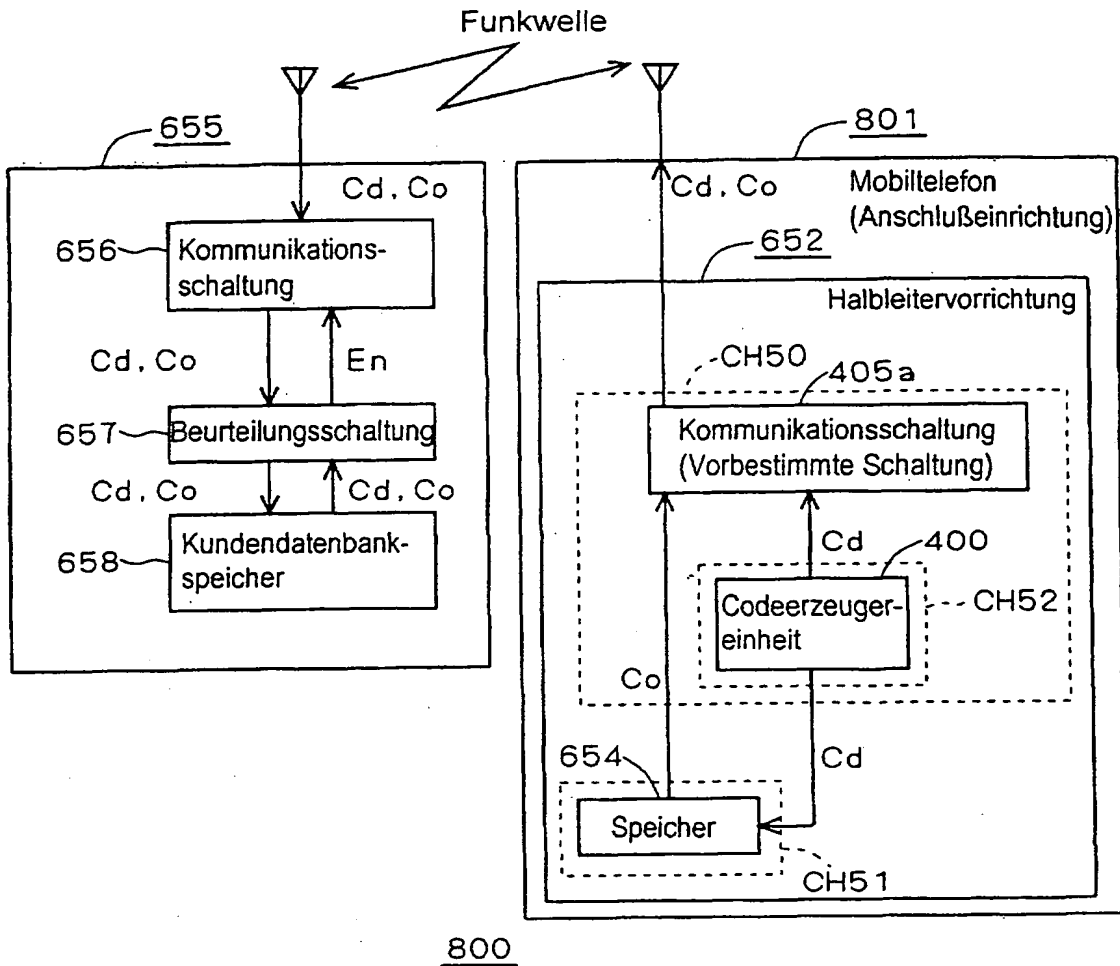


FIG. 21

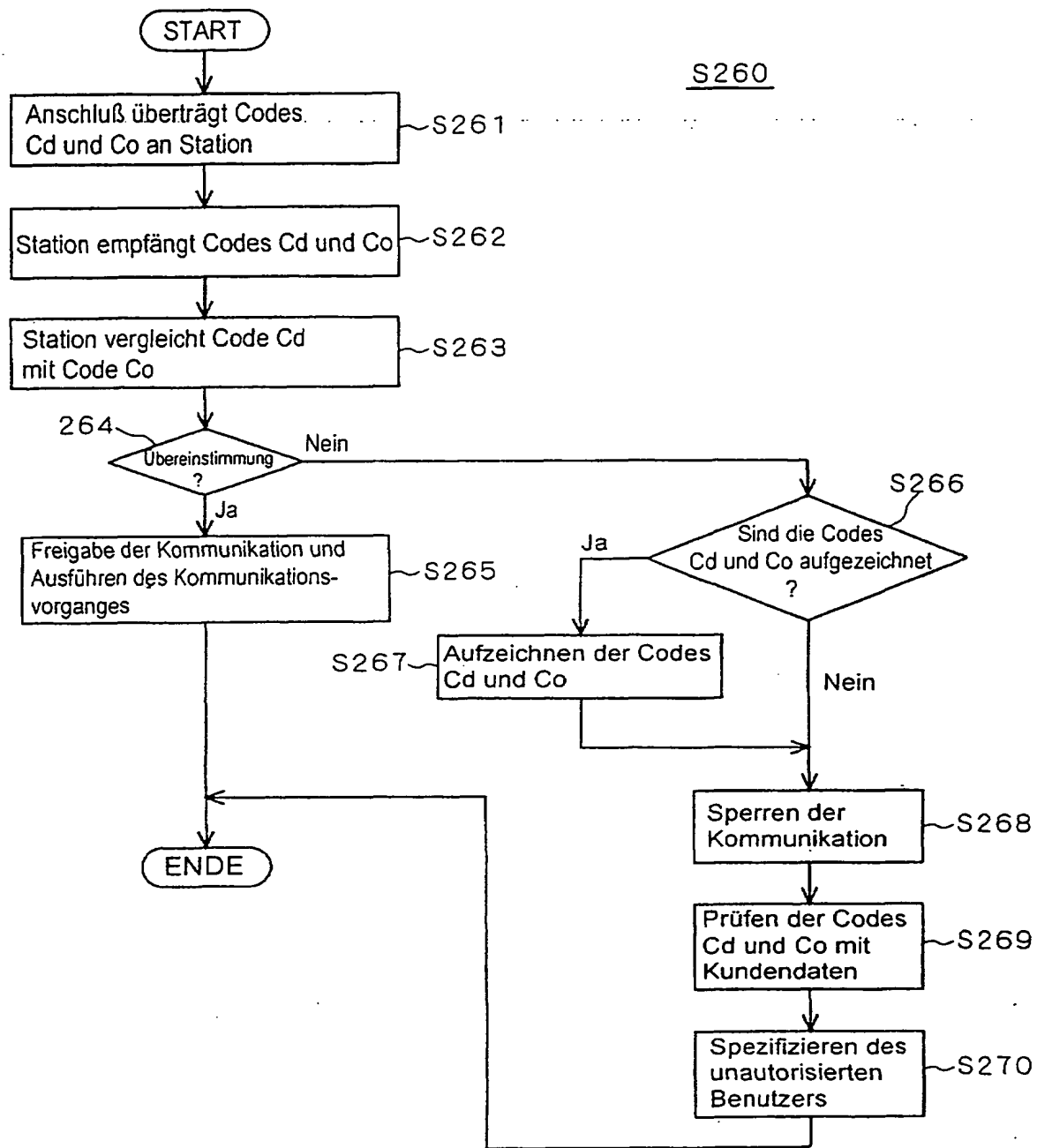
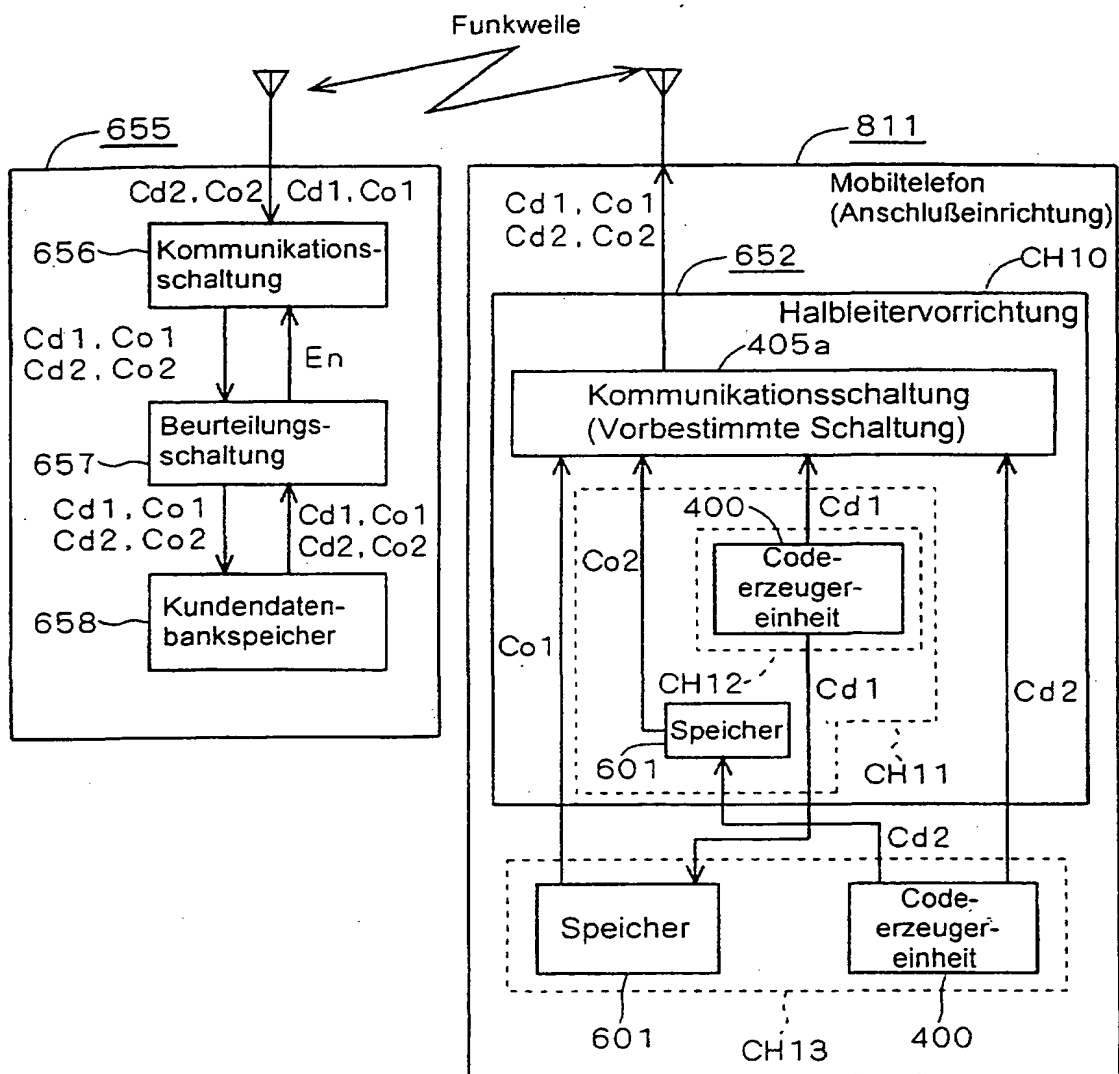


FIG. 22



810

FIG. 23

S280

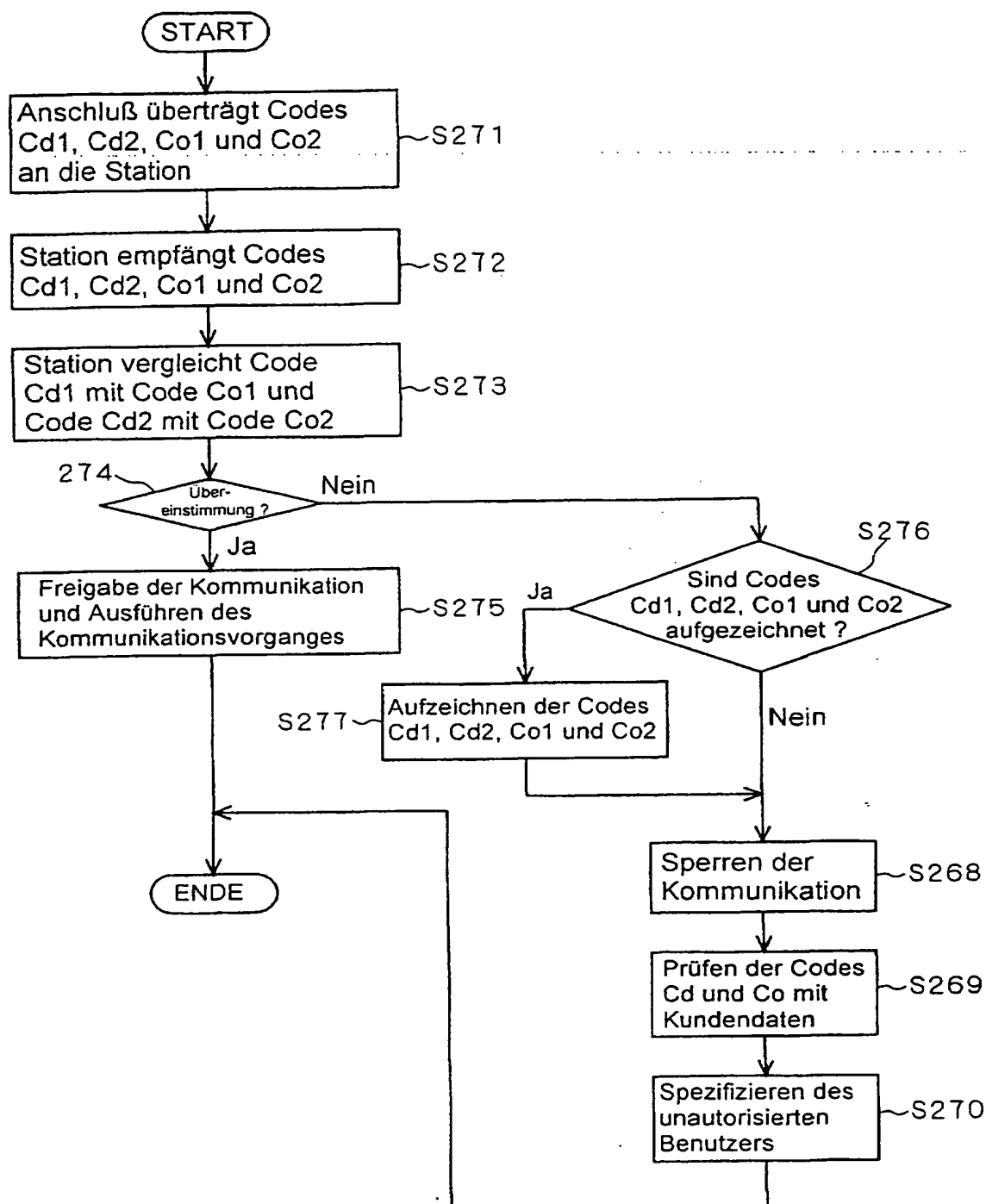


FIG. 24

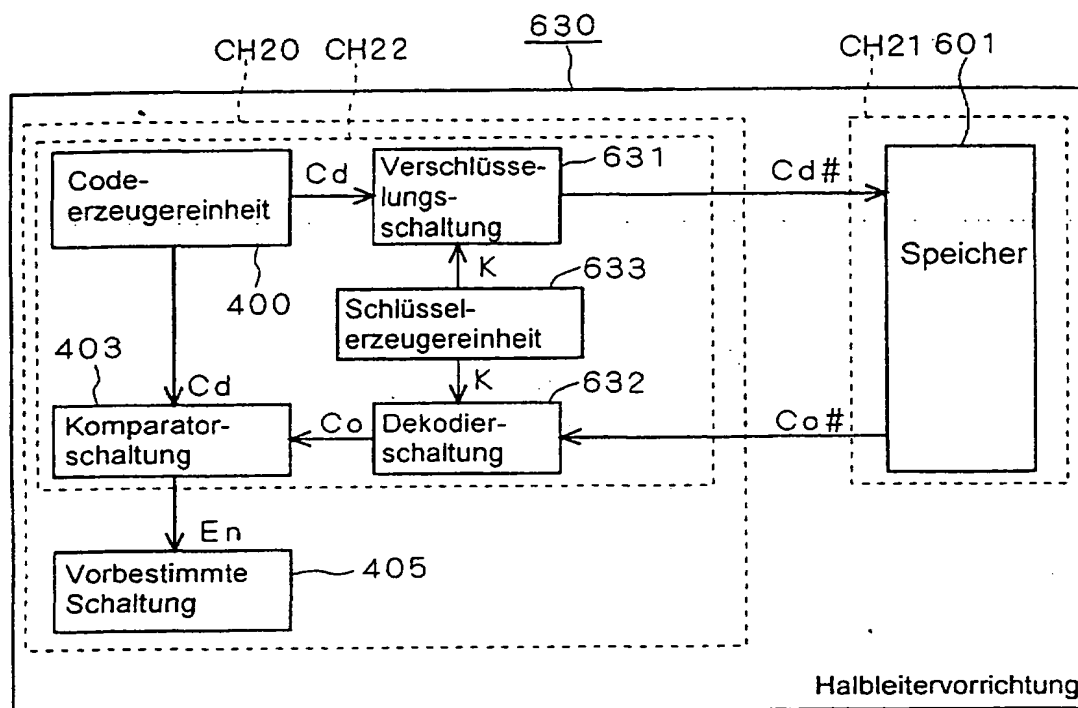


FIG. 25

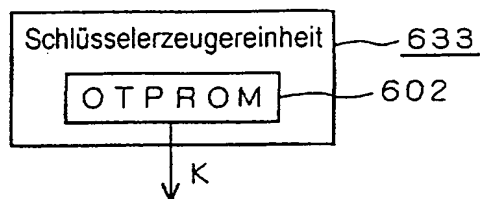


FIG. 26

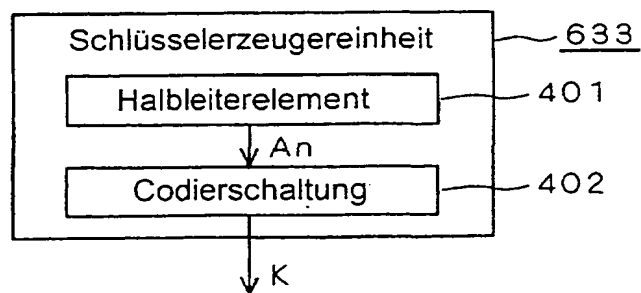


FIG. 27

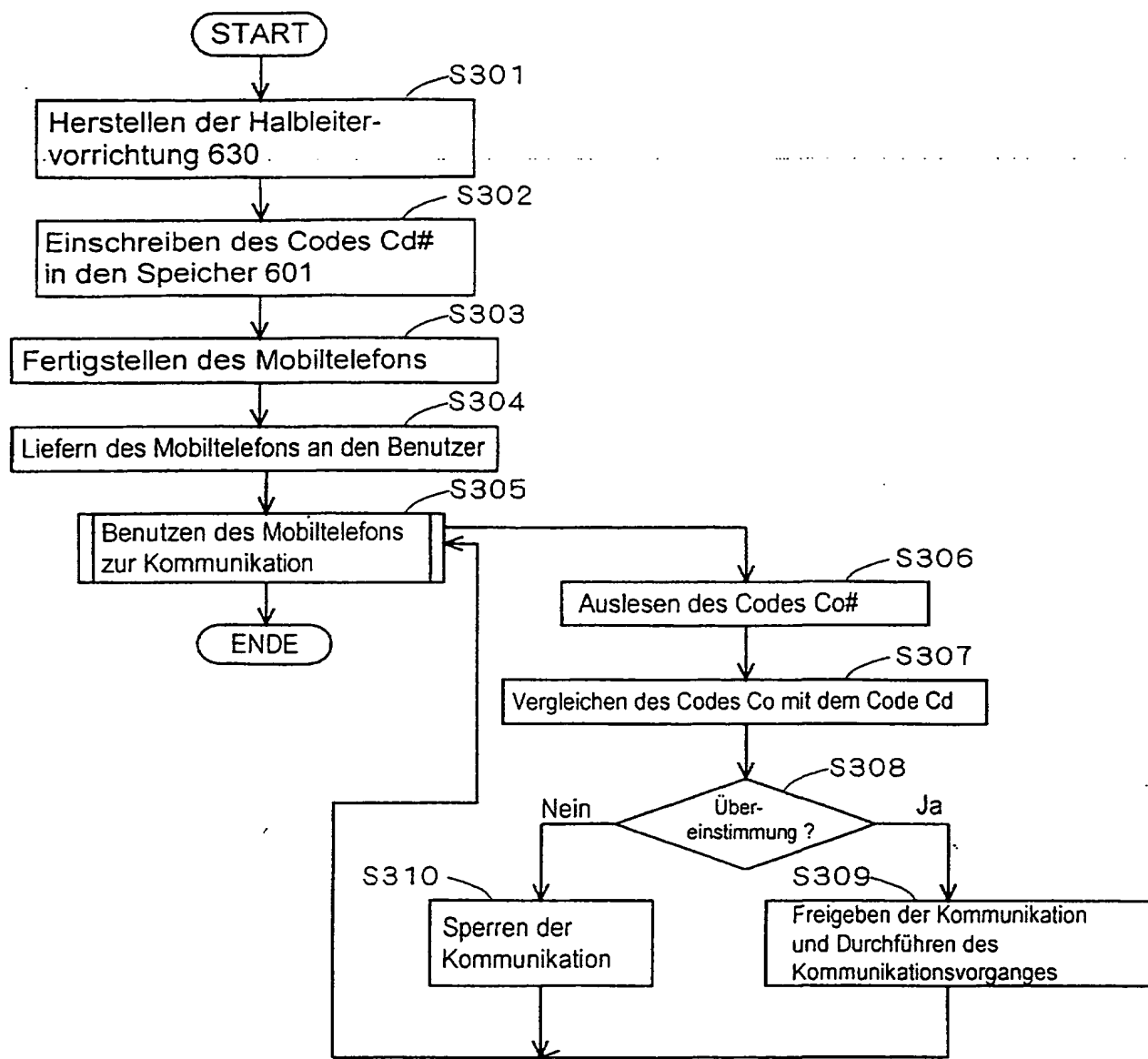


FIG. 28

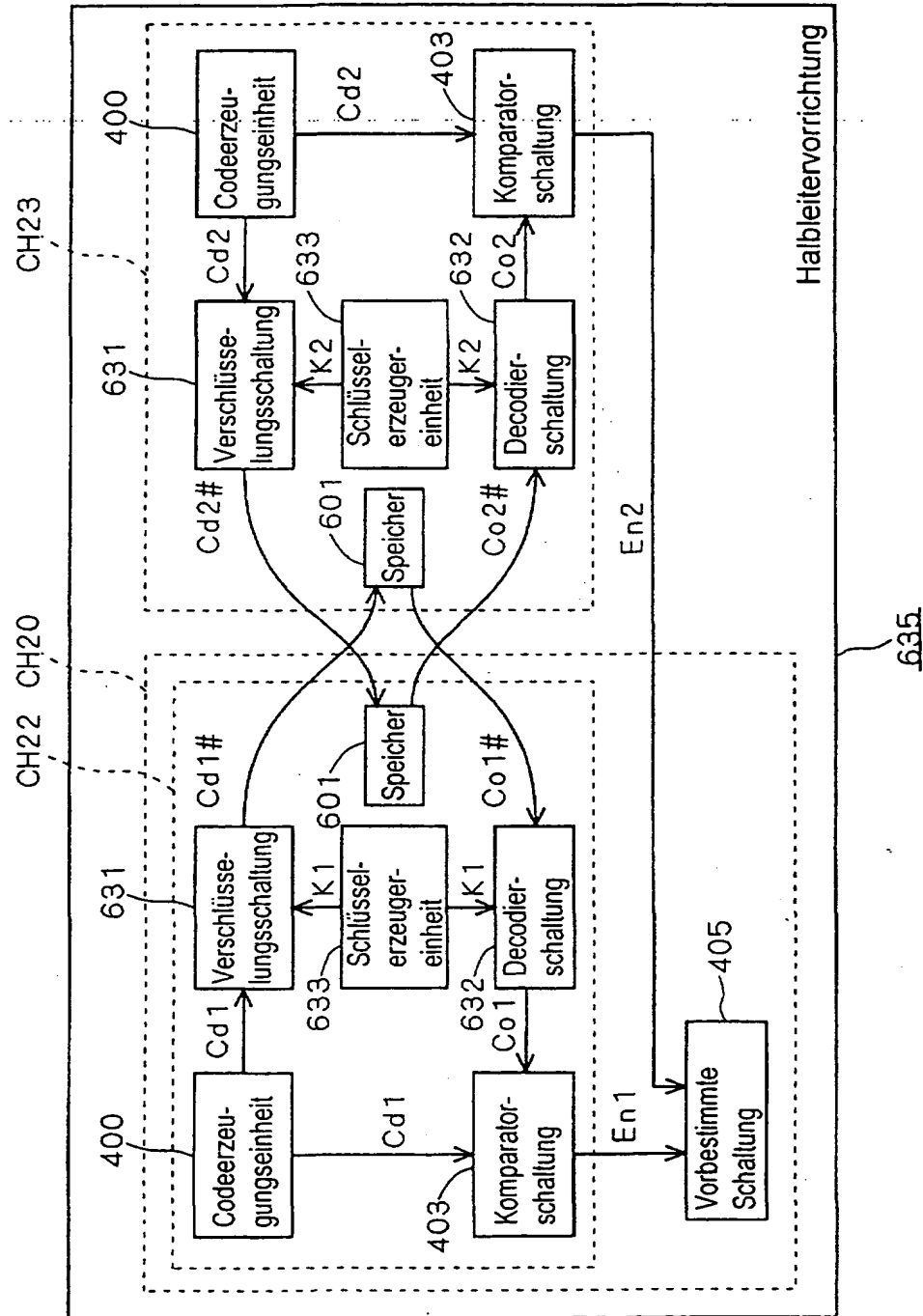


FIG. 29

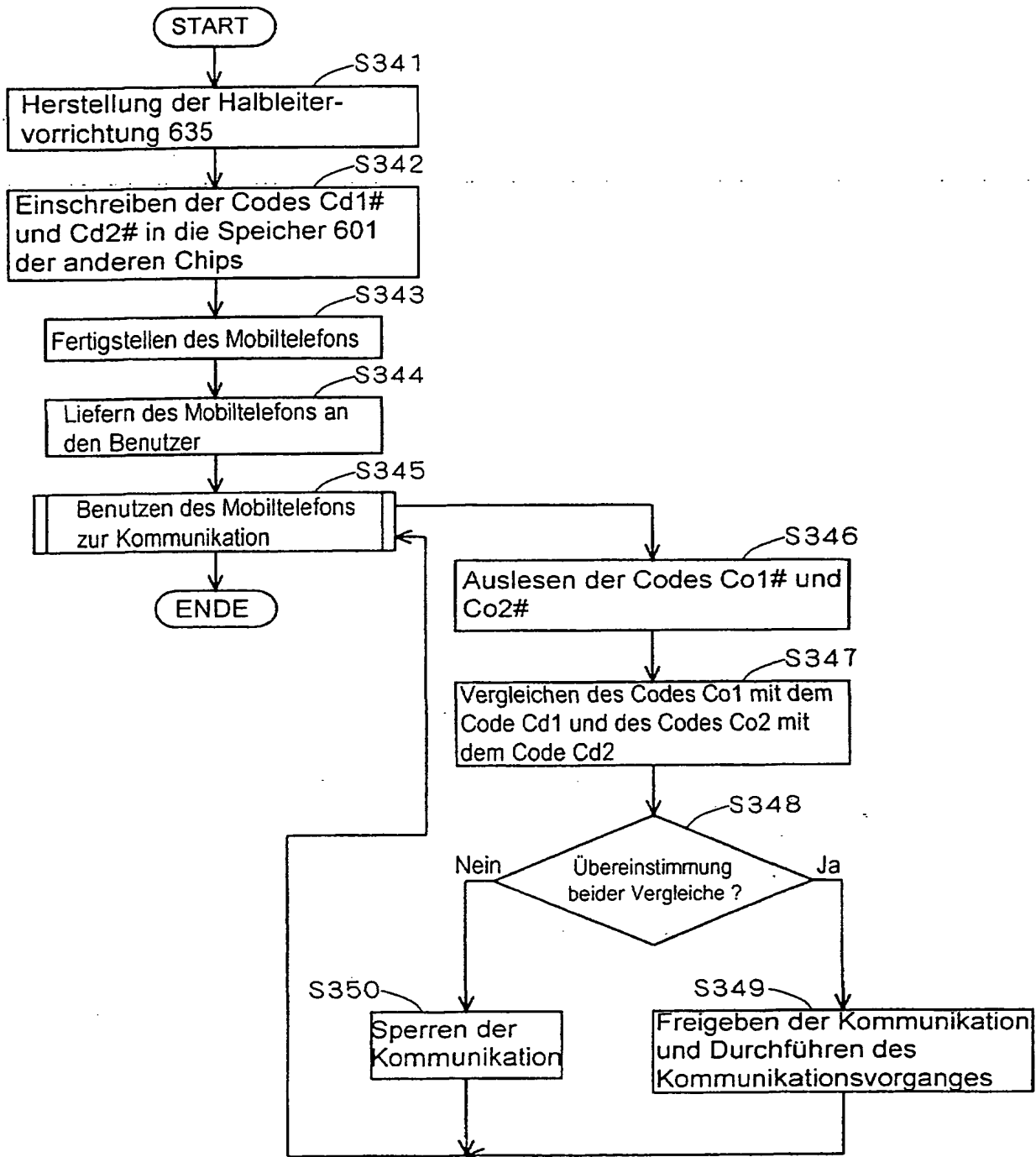


FIG. 30

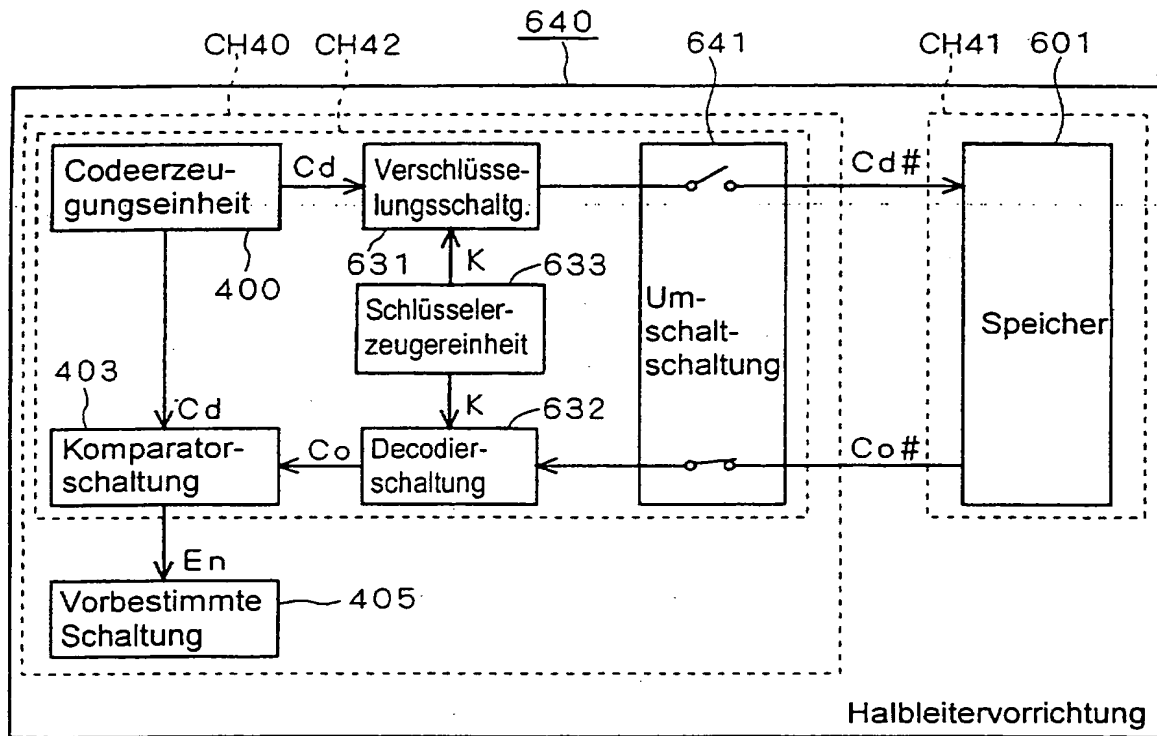


FIG. 31

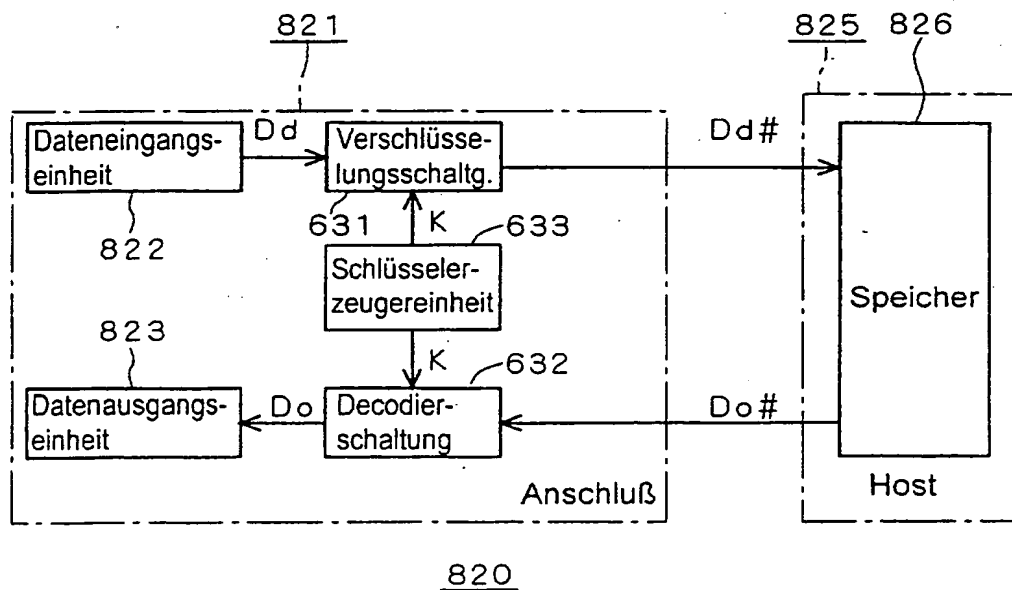
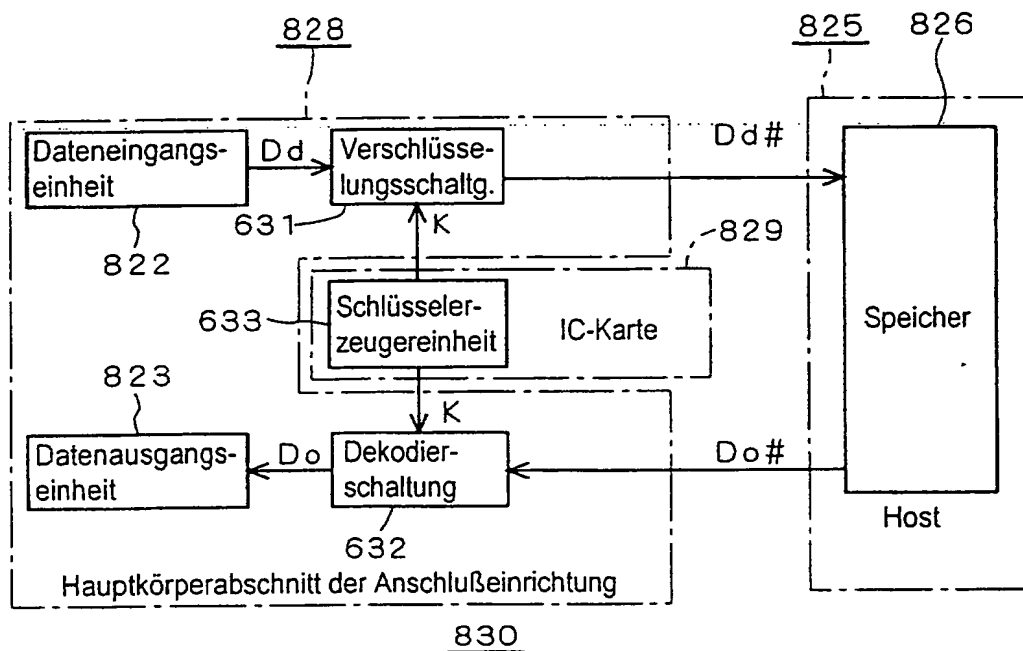


FIG. 32



F / G. 33

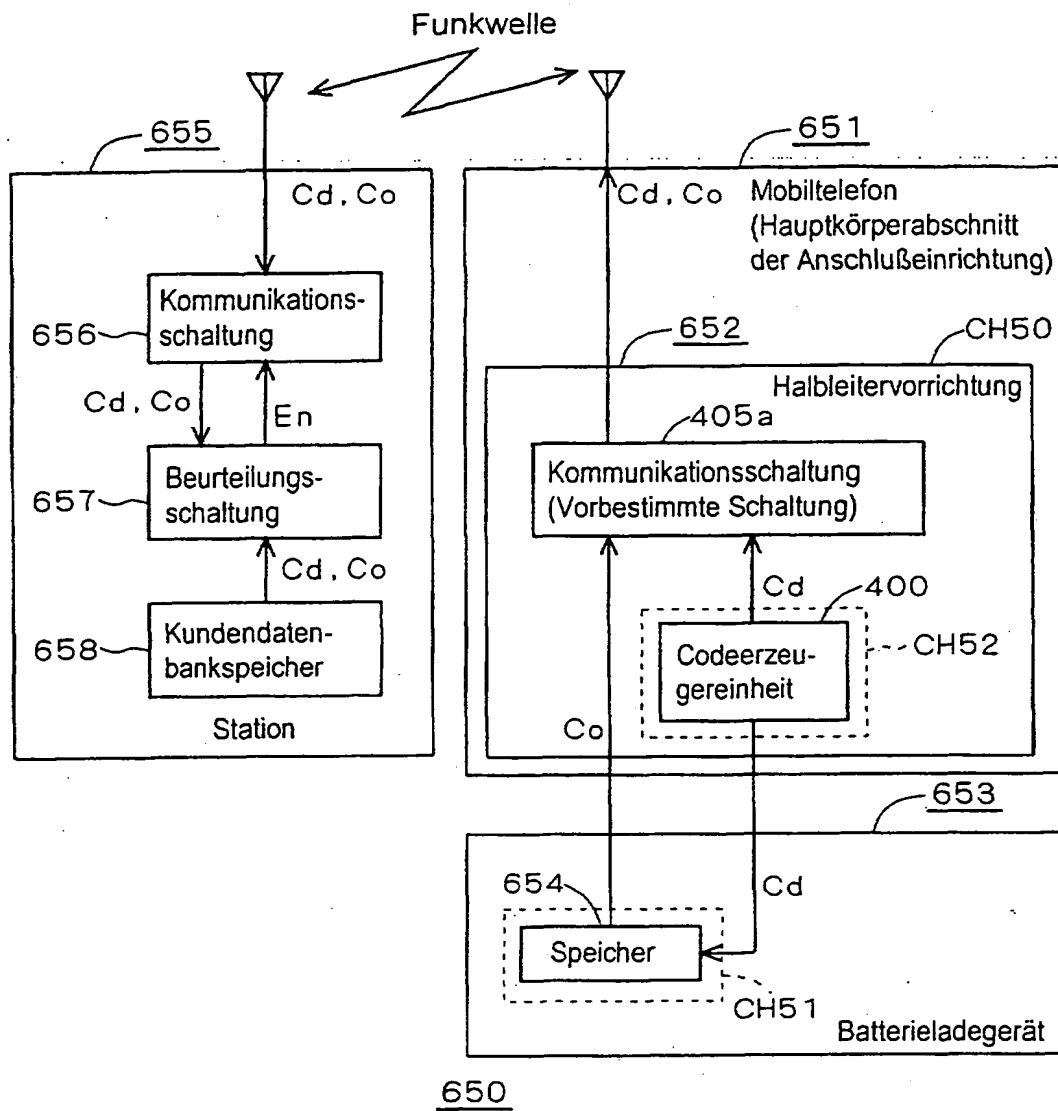


FIG. 34

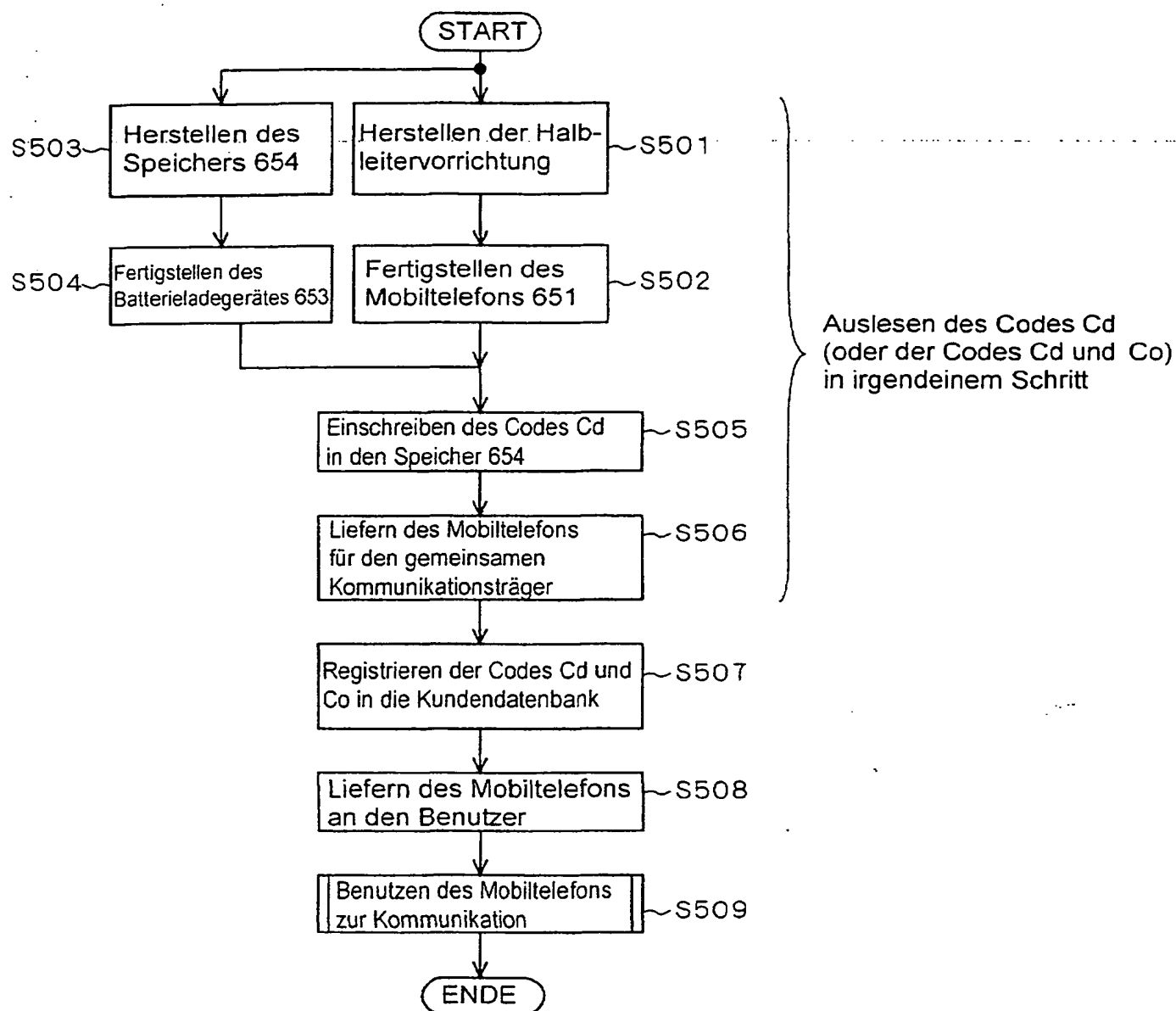


FIG. 35

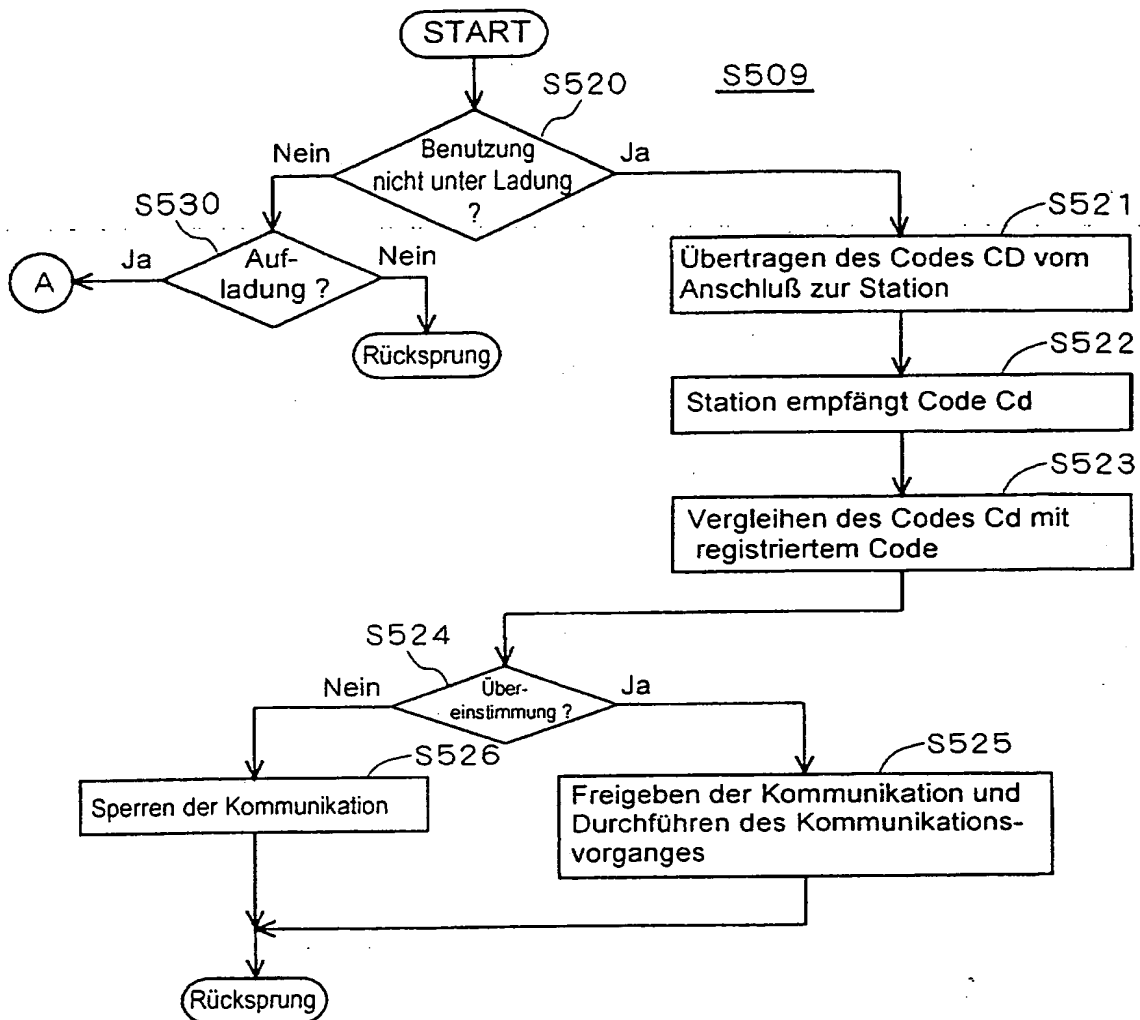


FIG. 36

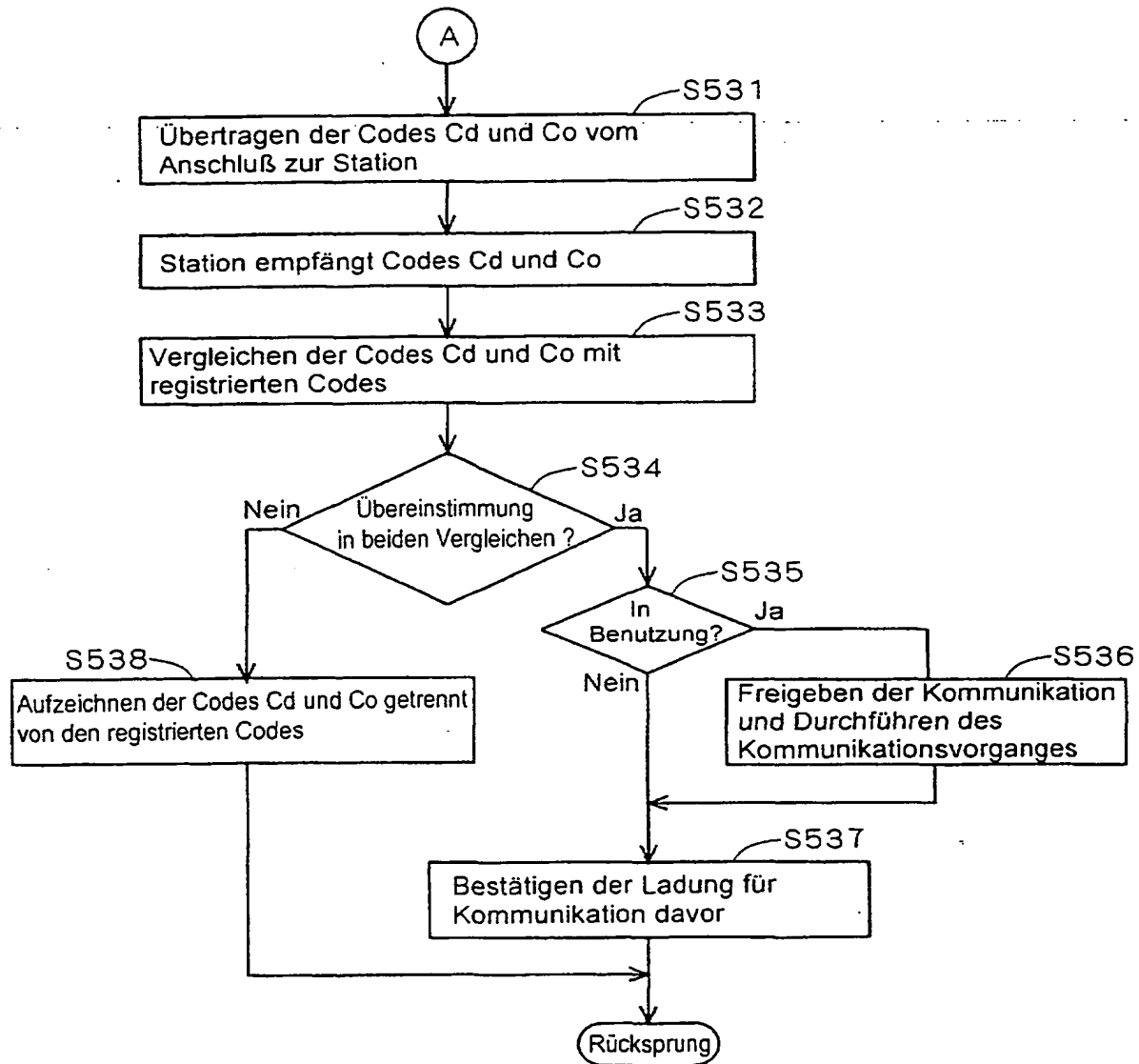


FIG. 37

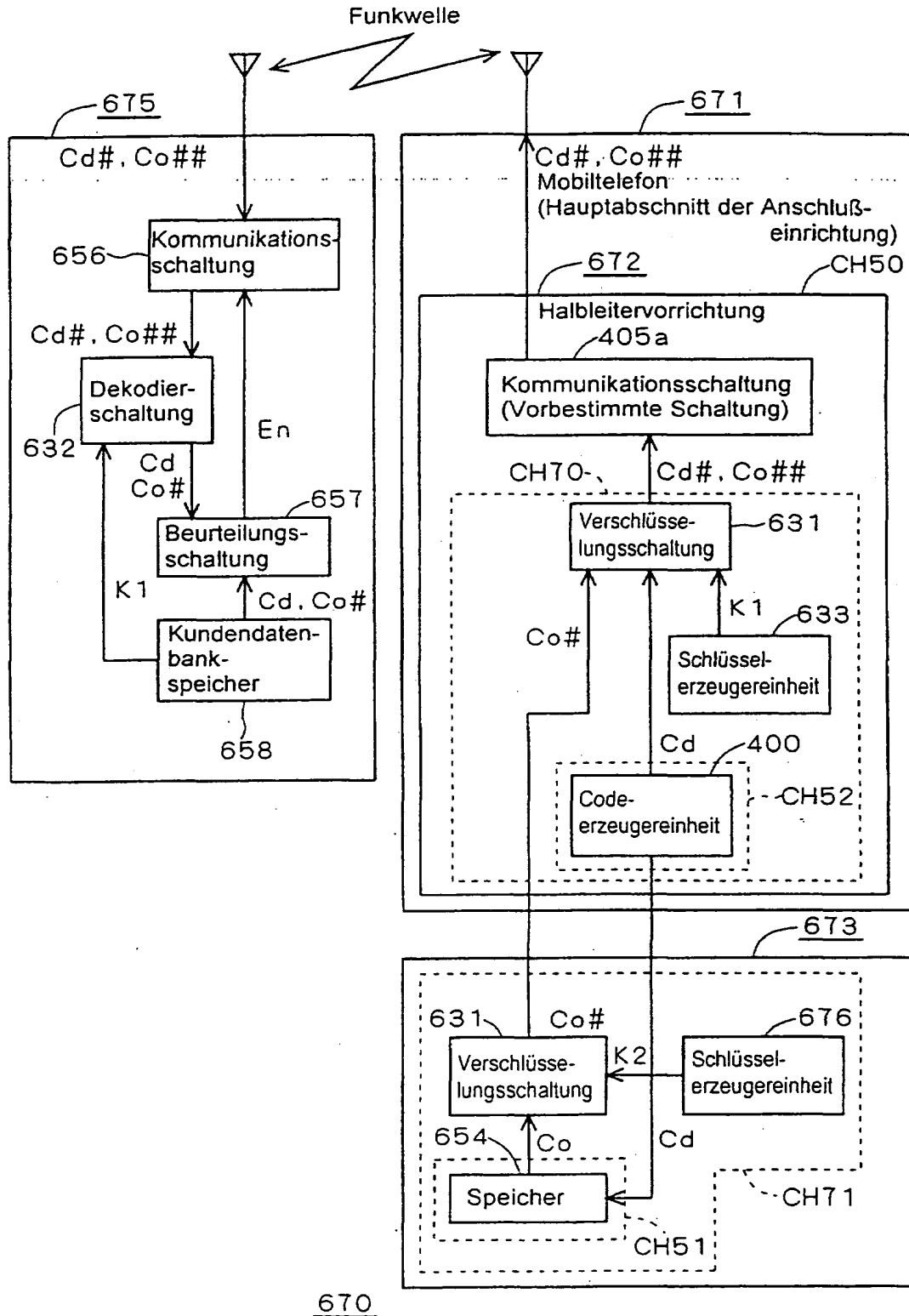


FIG. 38

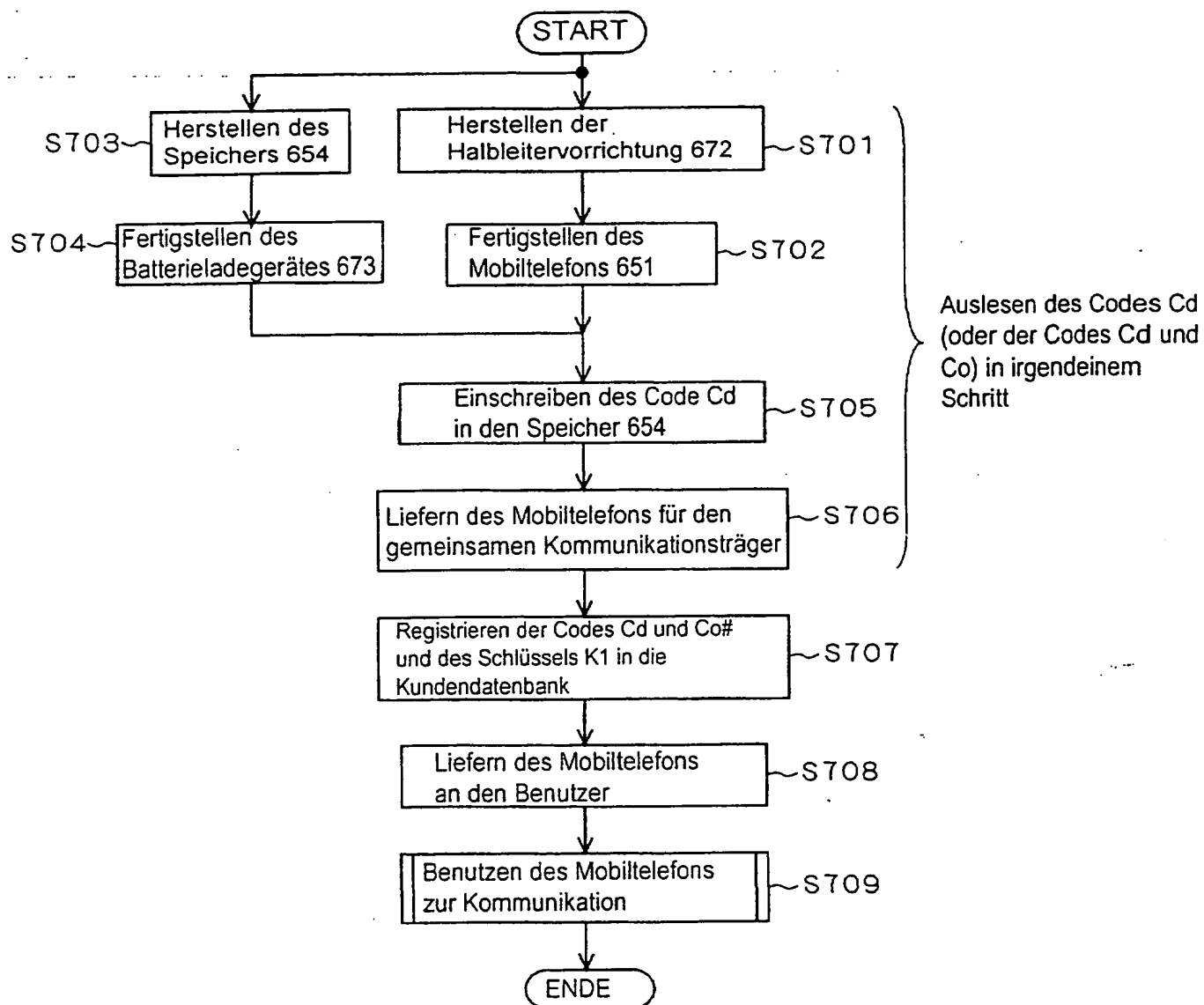


FIG. 39

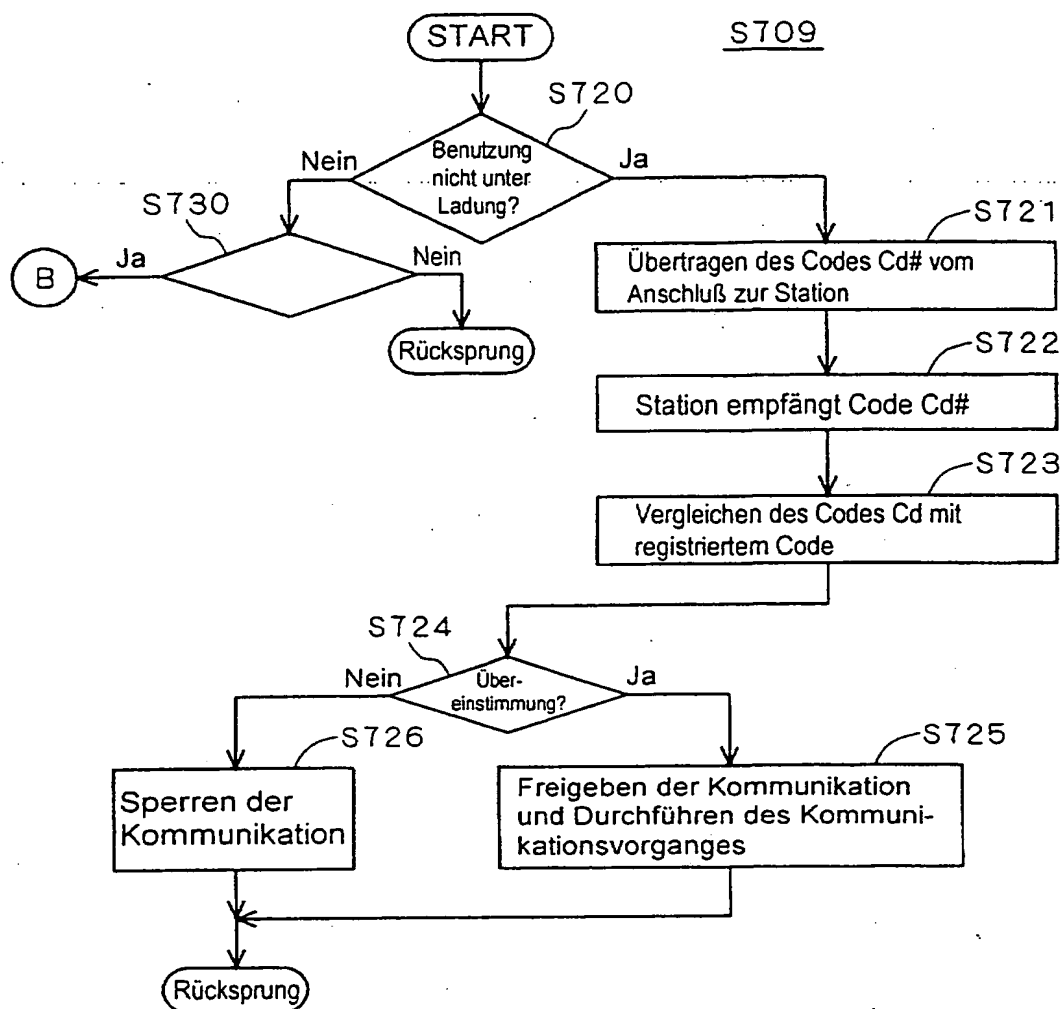


FIG. 40

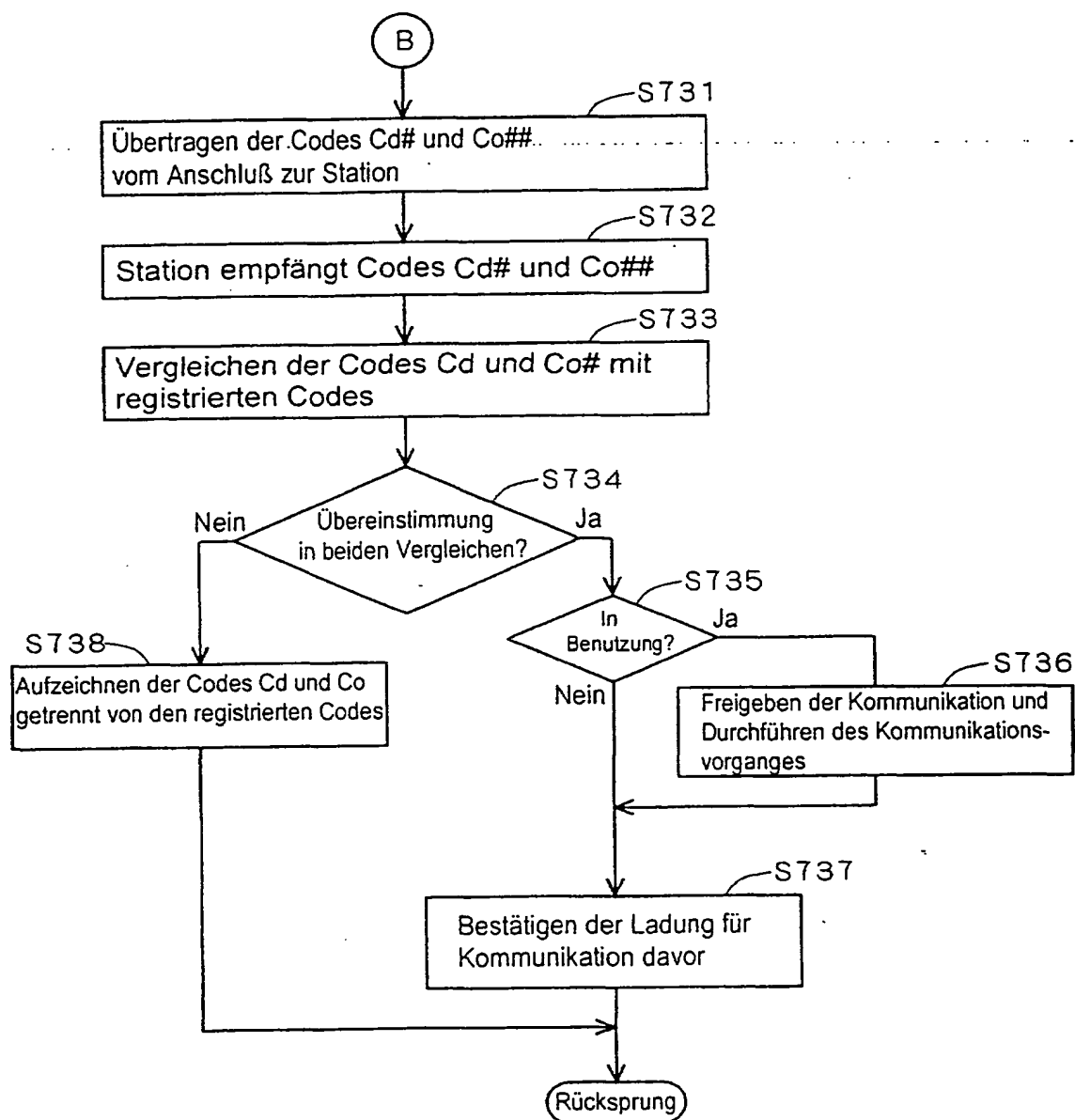


FIG. 41

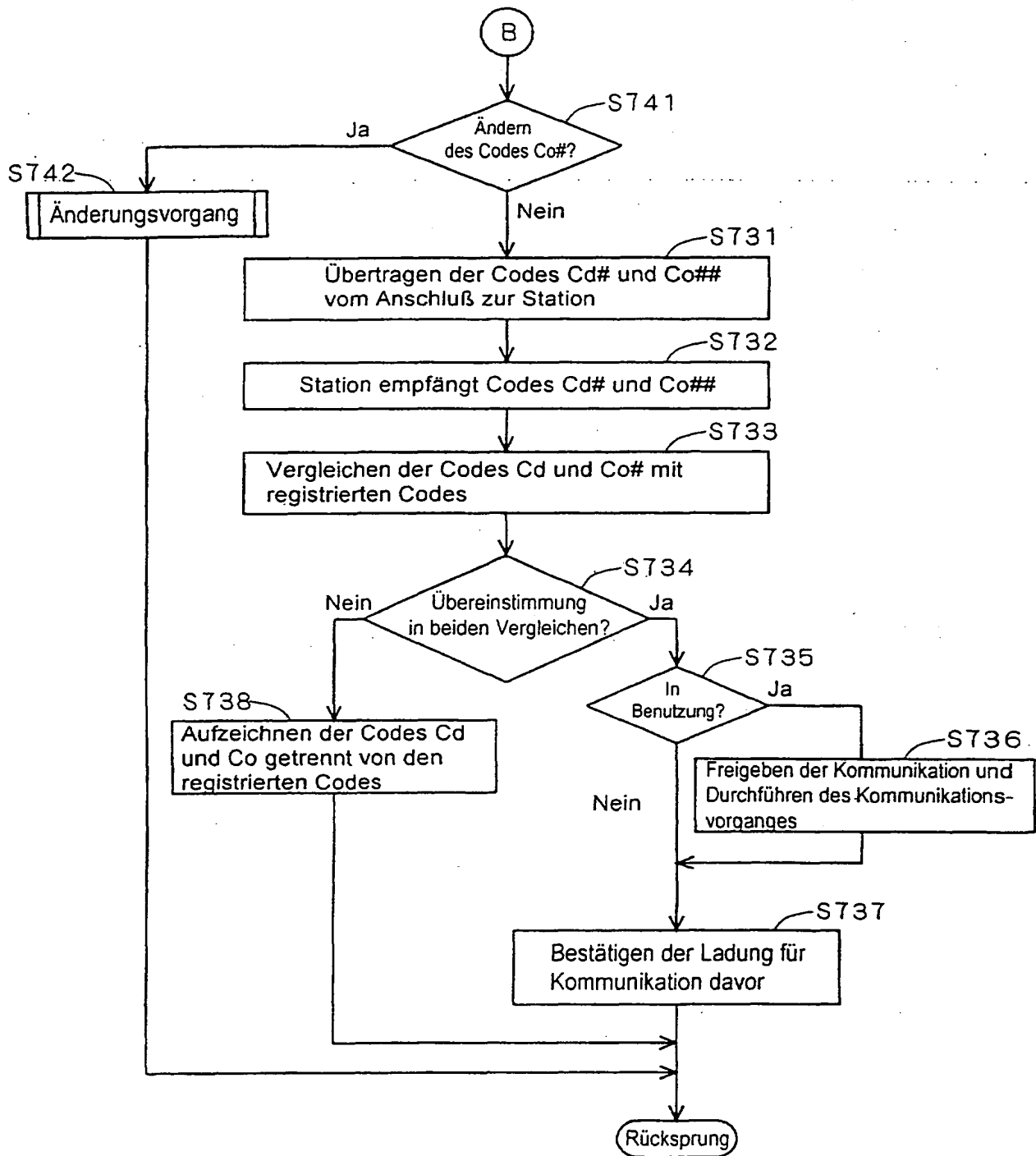


FIG. 42

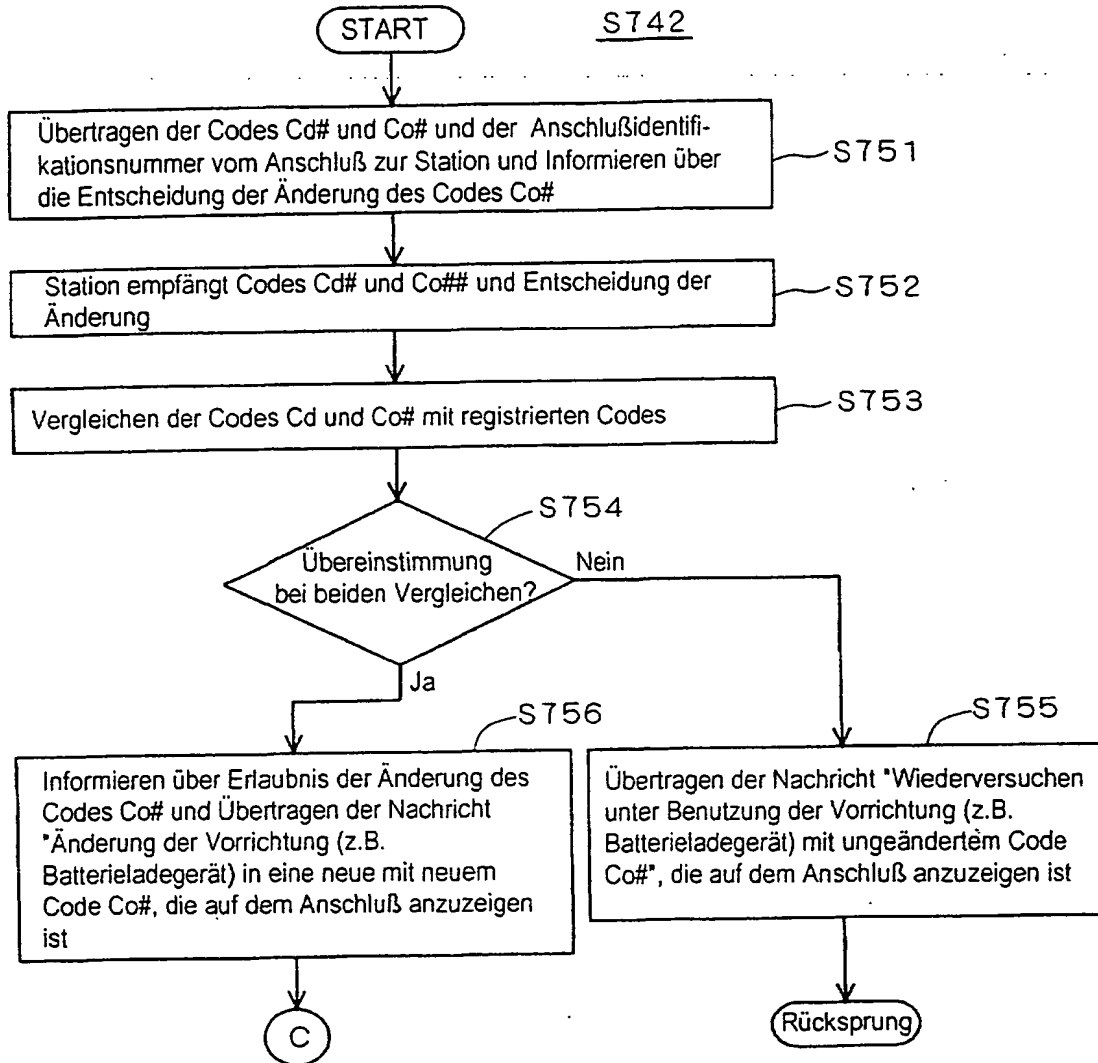


FIG. 43

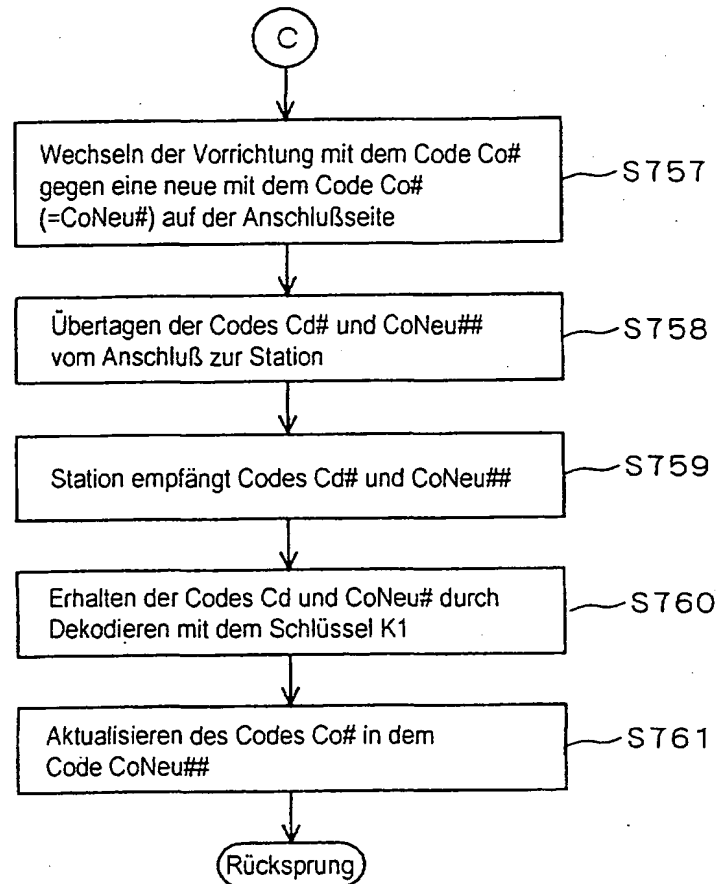


FIG. 44

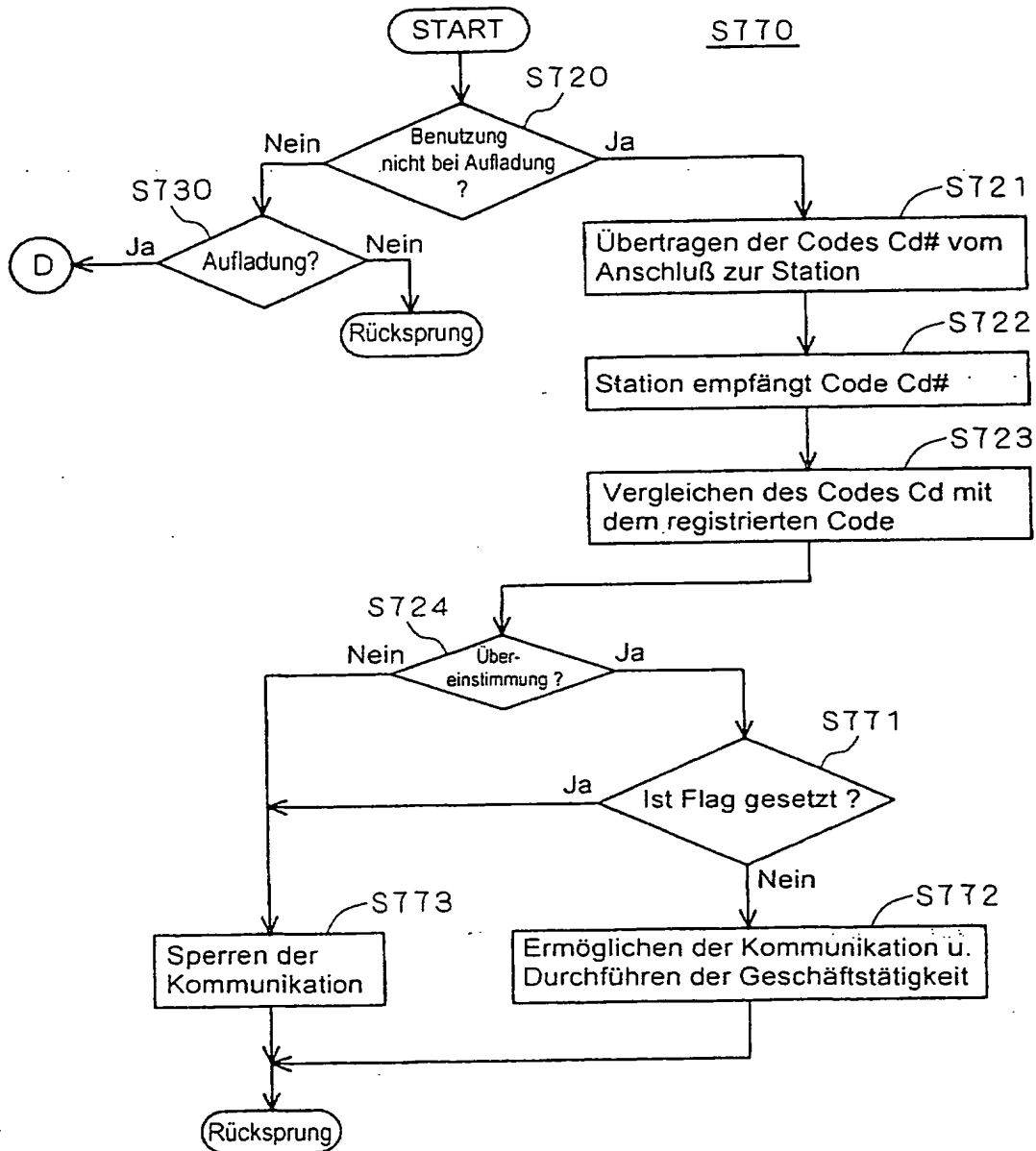


FIG. 45

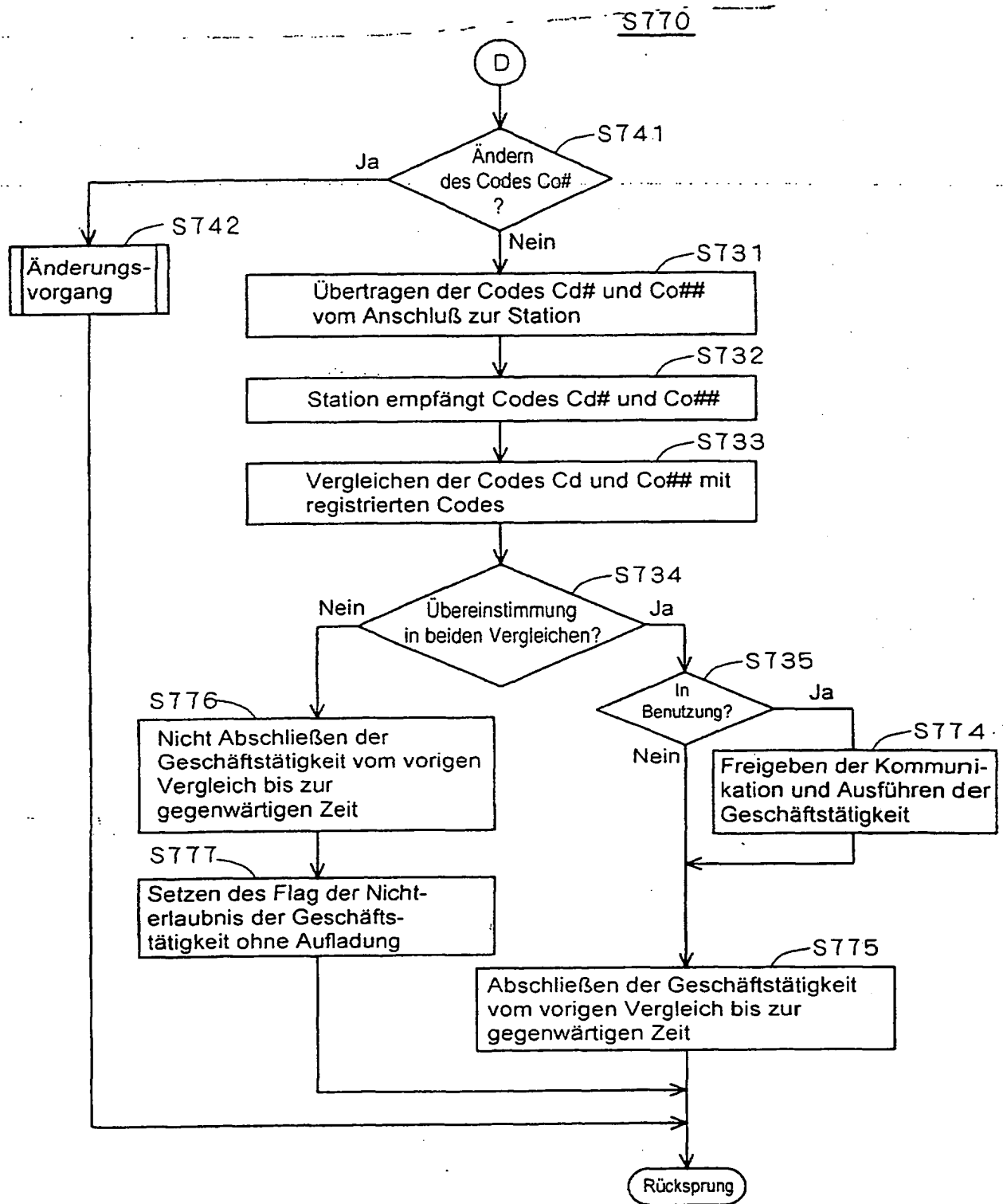


FIG. 47

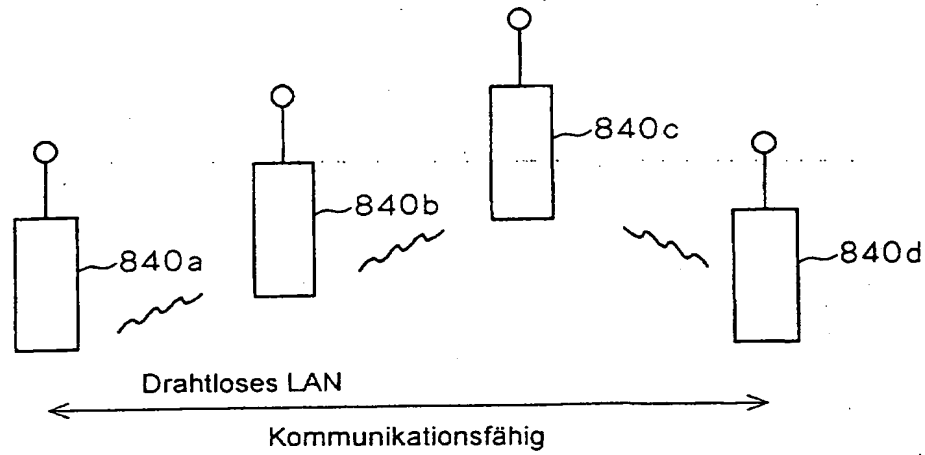


FIG. 48

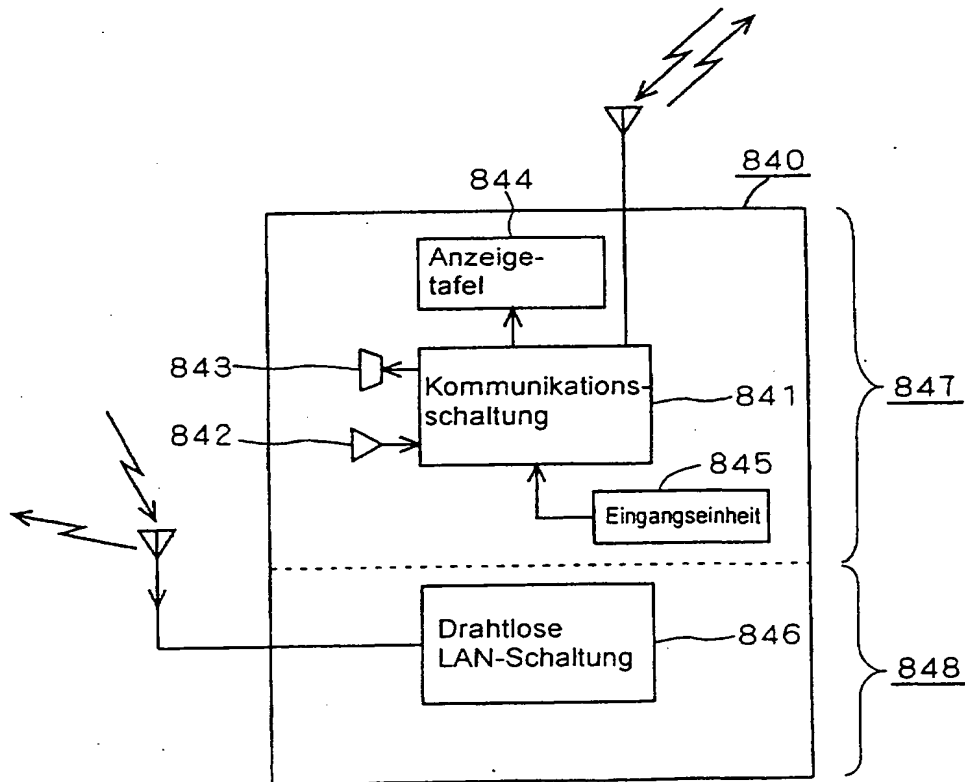


FIG. 49

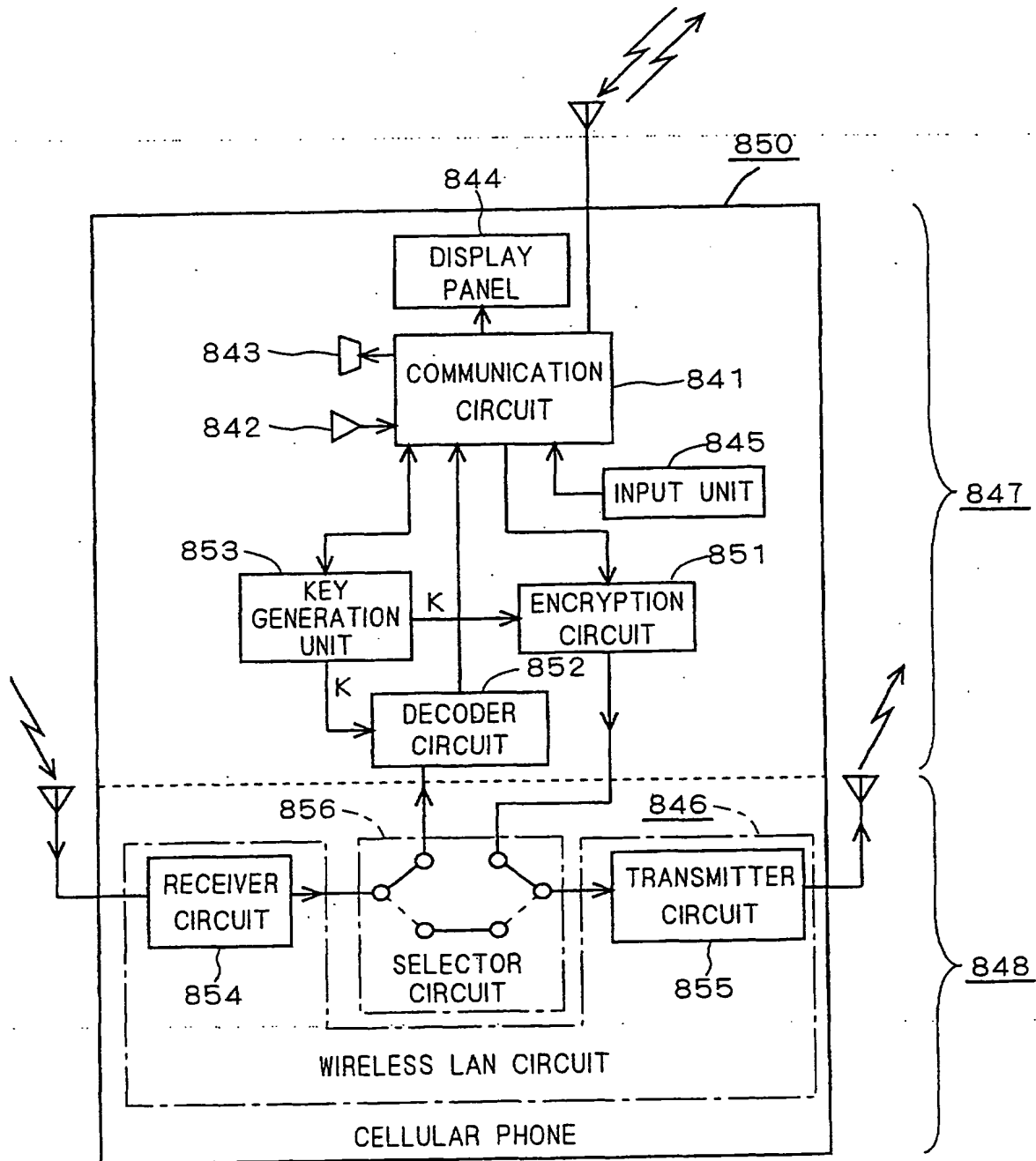


FIG. 50

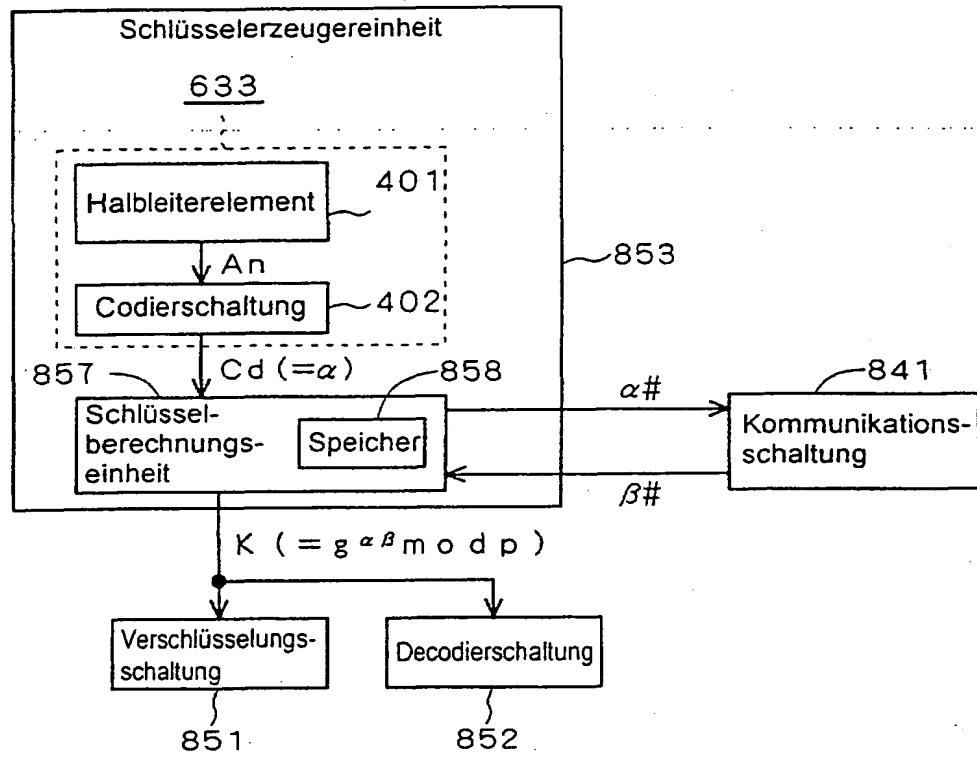


FIG. 51

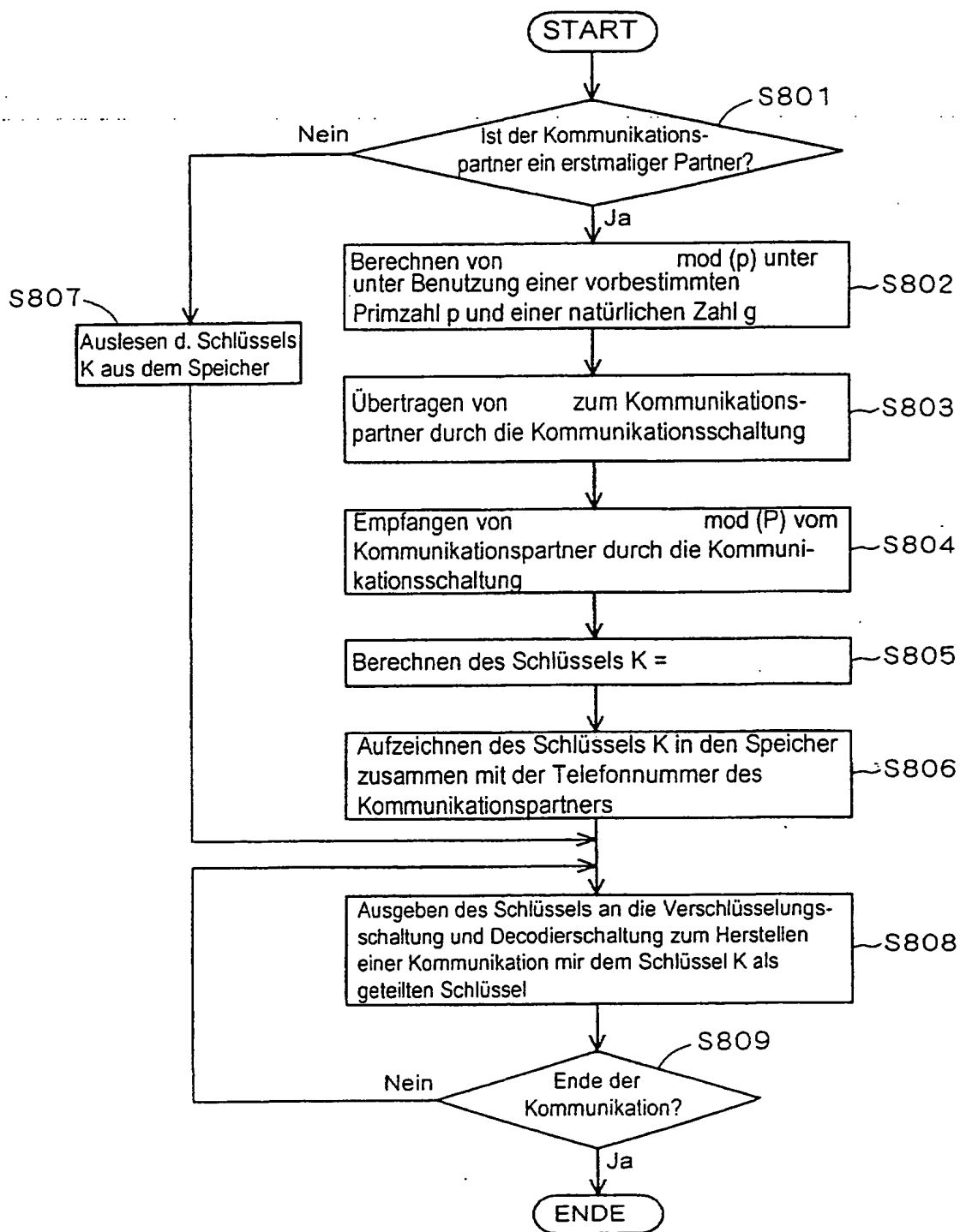


FIG. 52

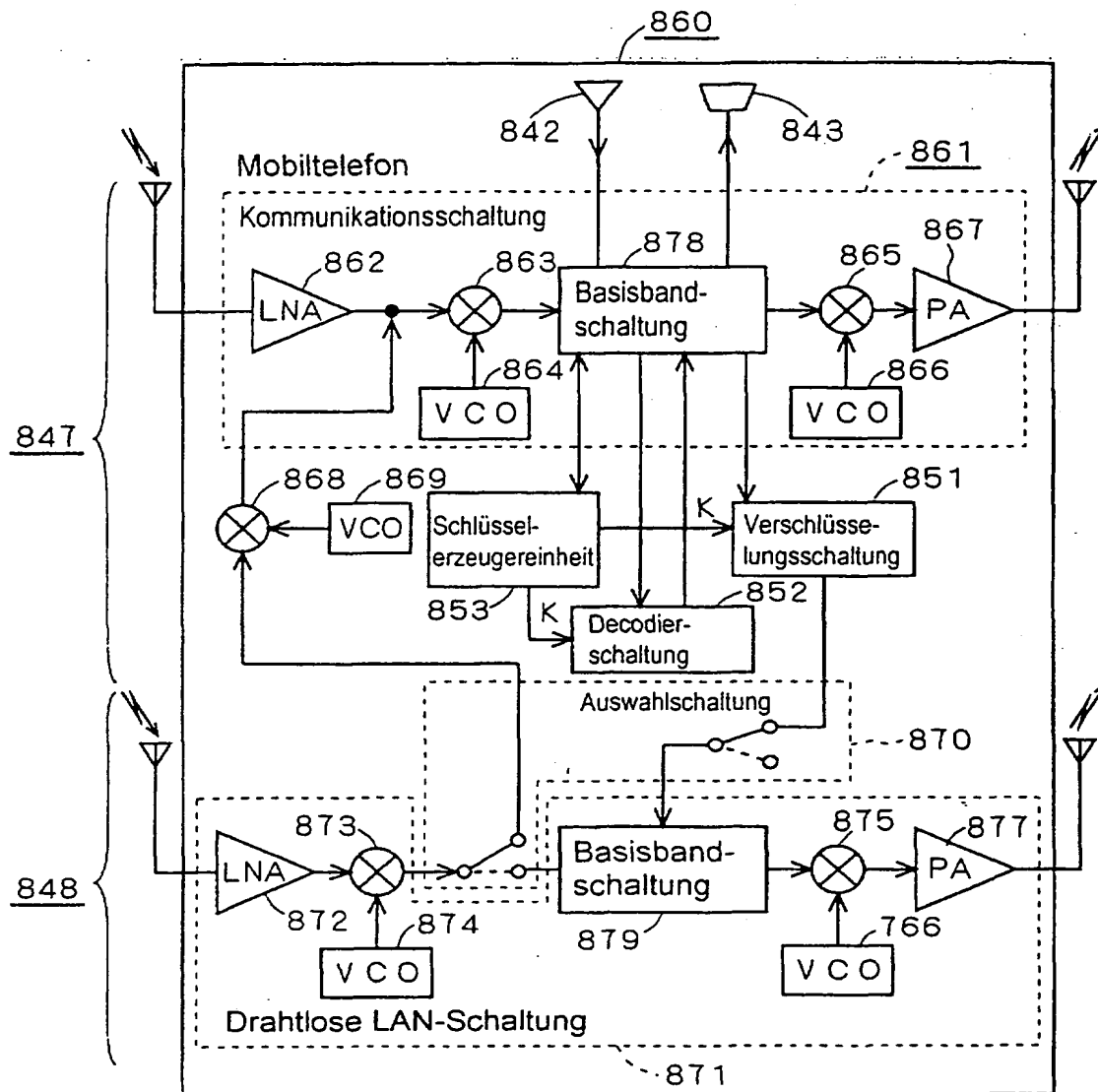


FIG. 53

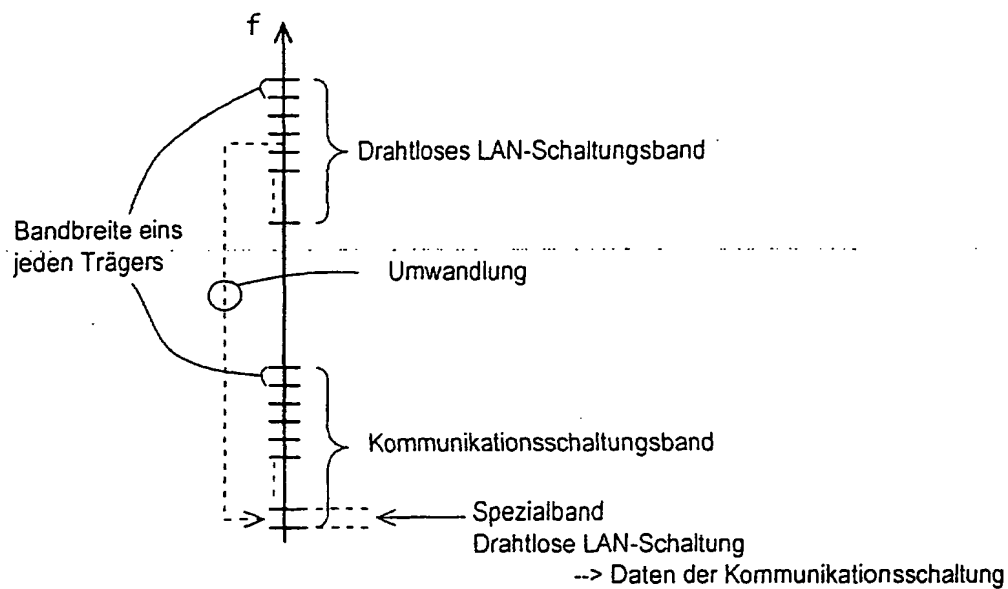


FIG. 54

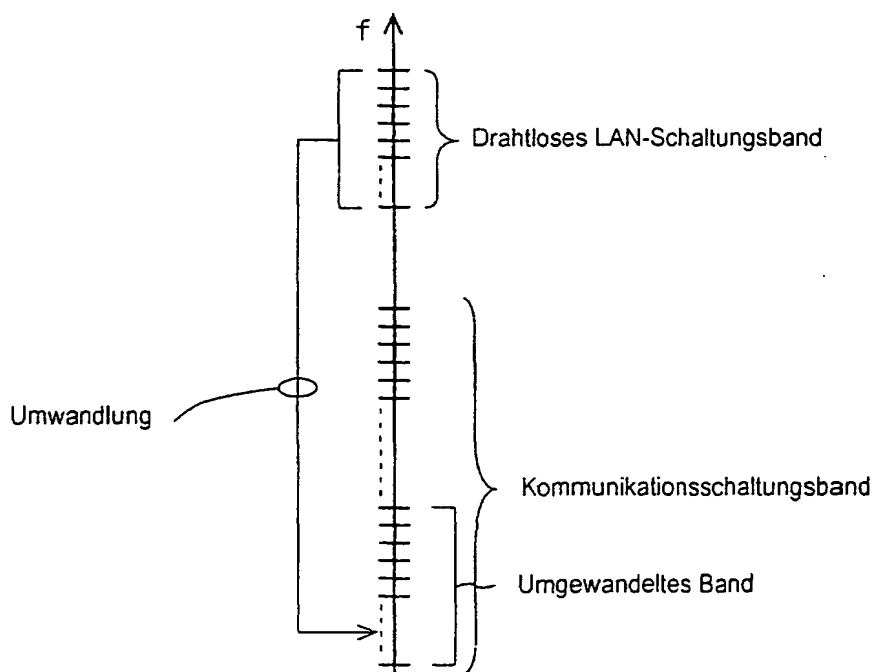


FIG. 55

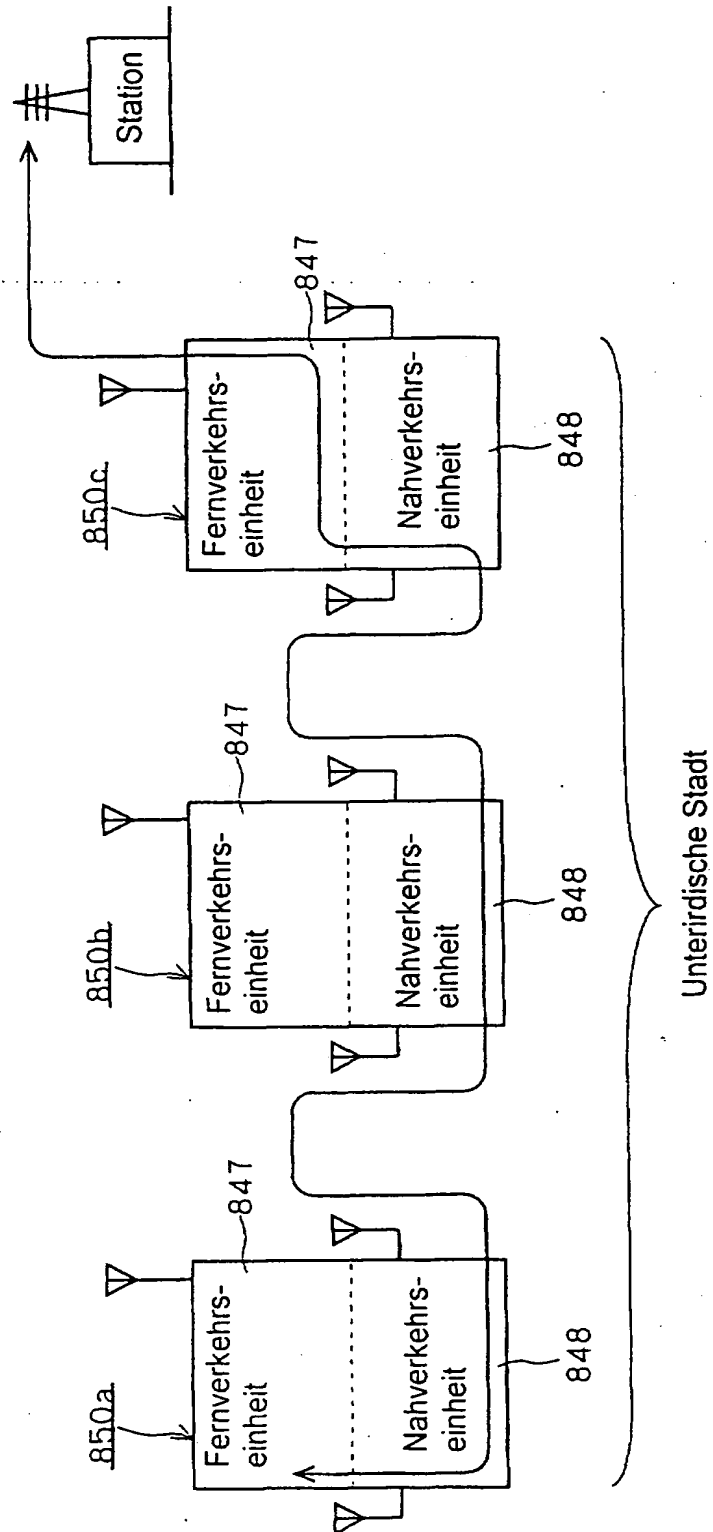


FIG. 56

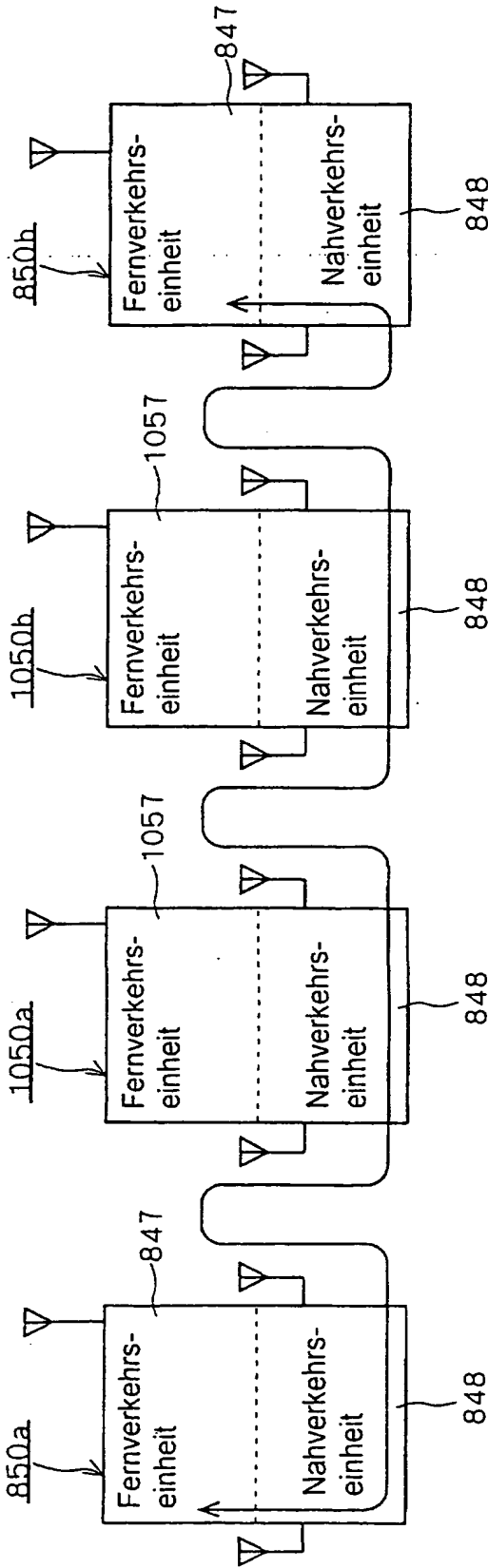


FIG. 57

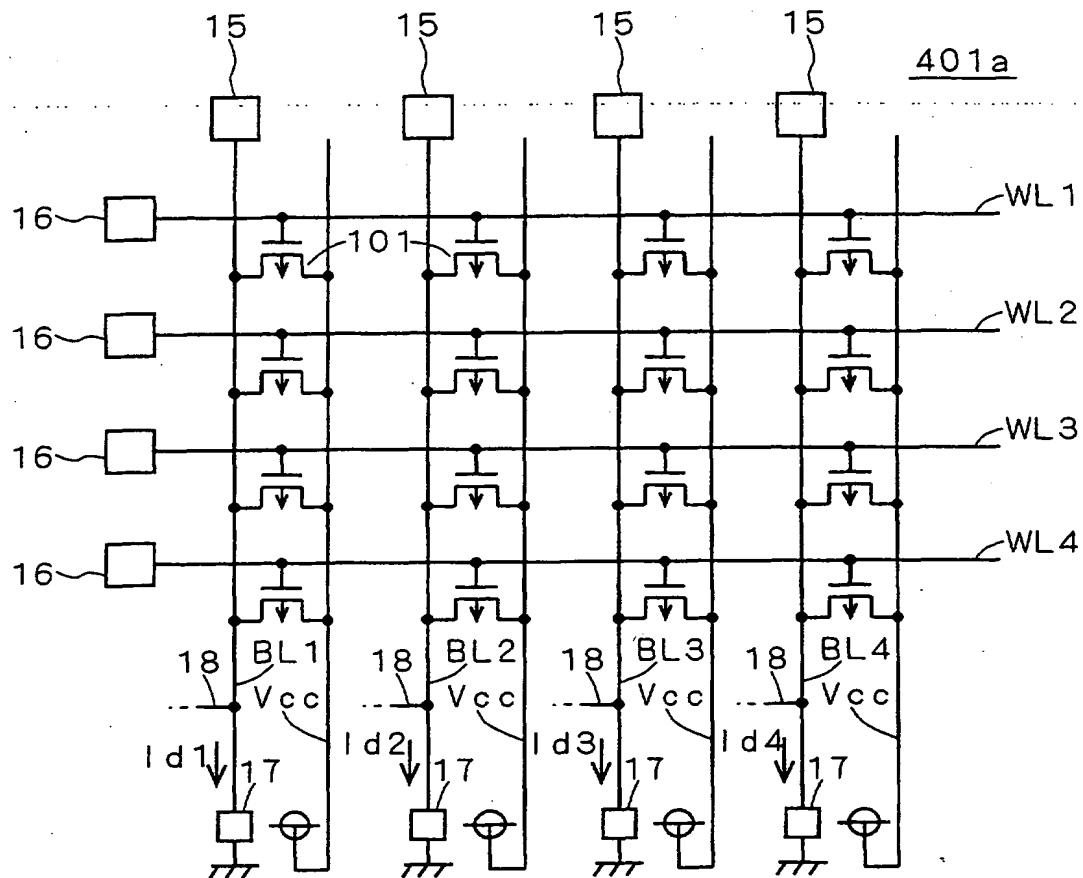


FIG. 58

	BL 1	BL 2	BL 3	BL 4
WL 1	1	1	0	0
WL 2	1	0	1	0
WL 3	0	0	0	1
WL 4	0	1	0	0

FIG. 59

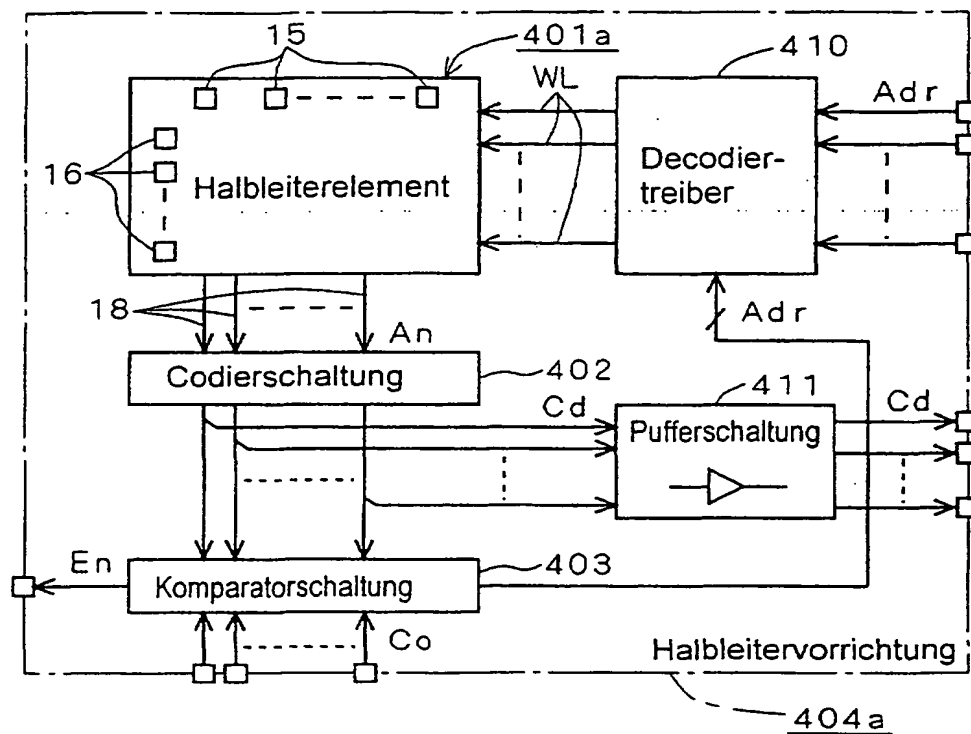
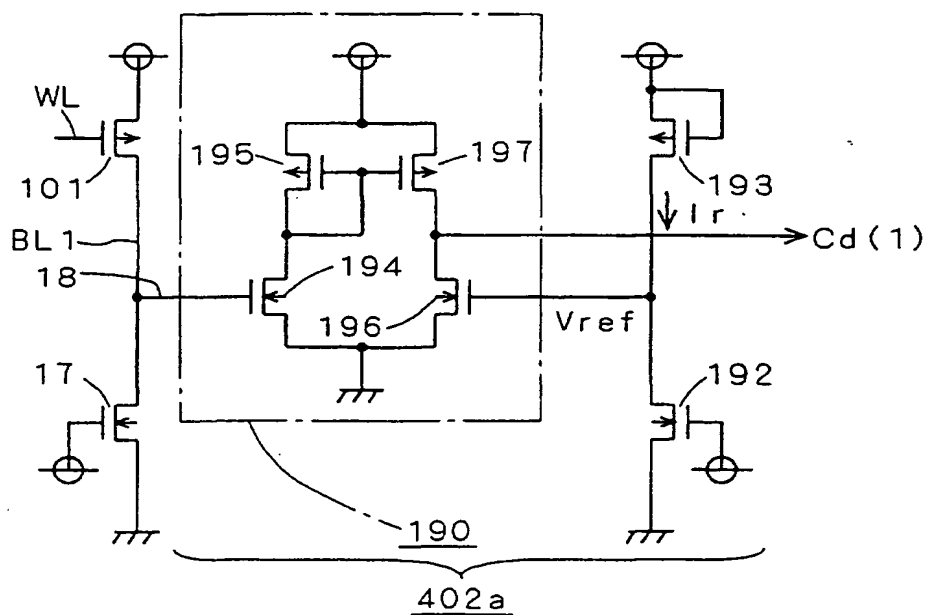


FIG. 60



F / G. 61

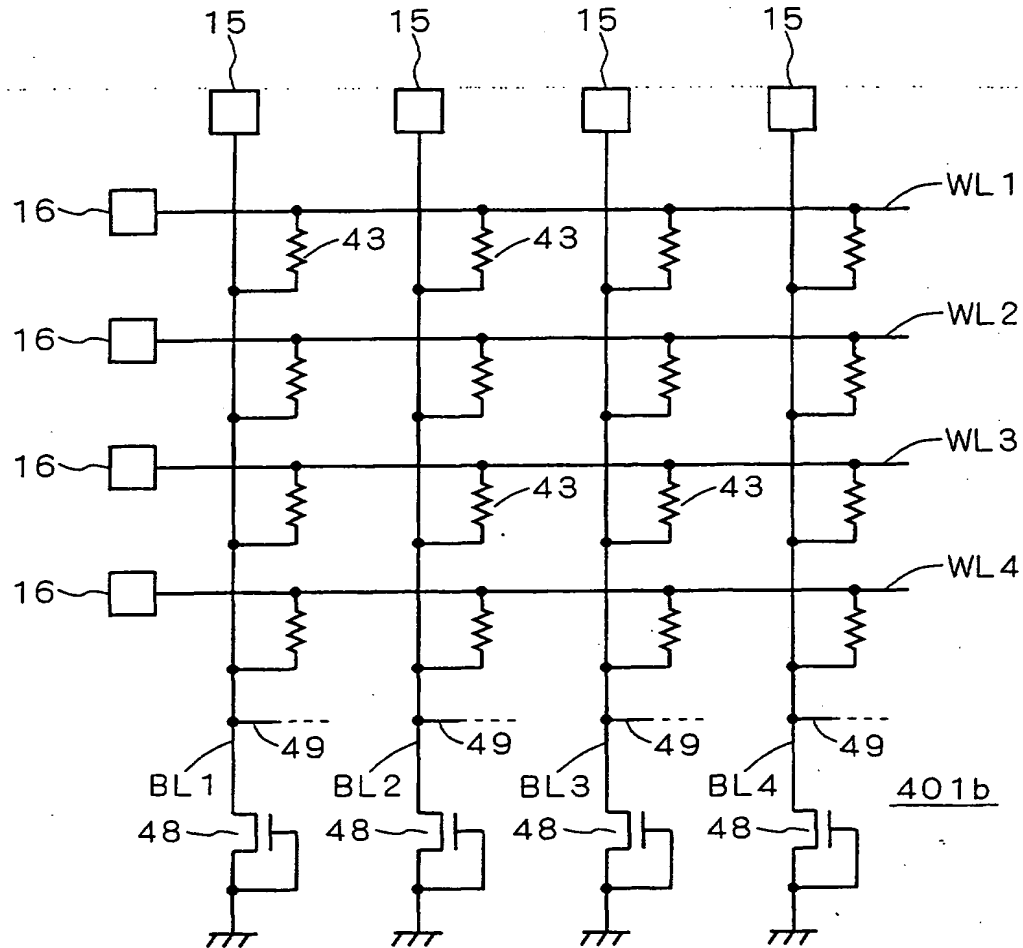


FIG. 62

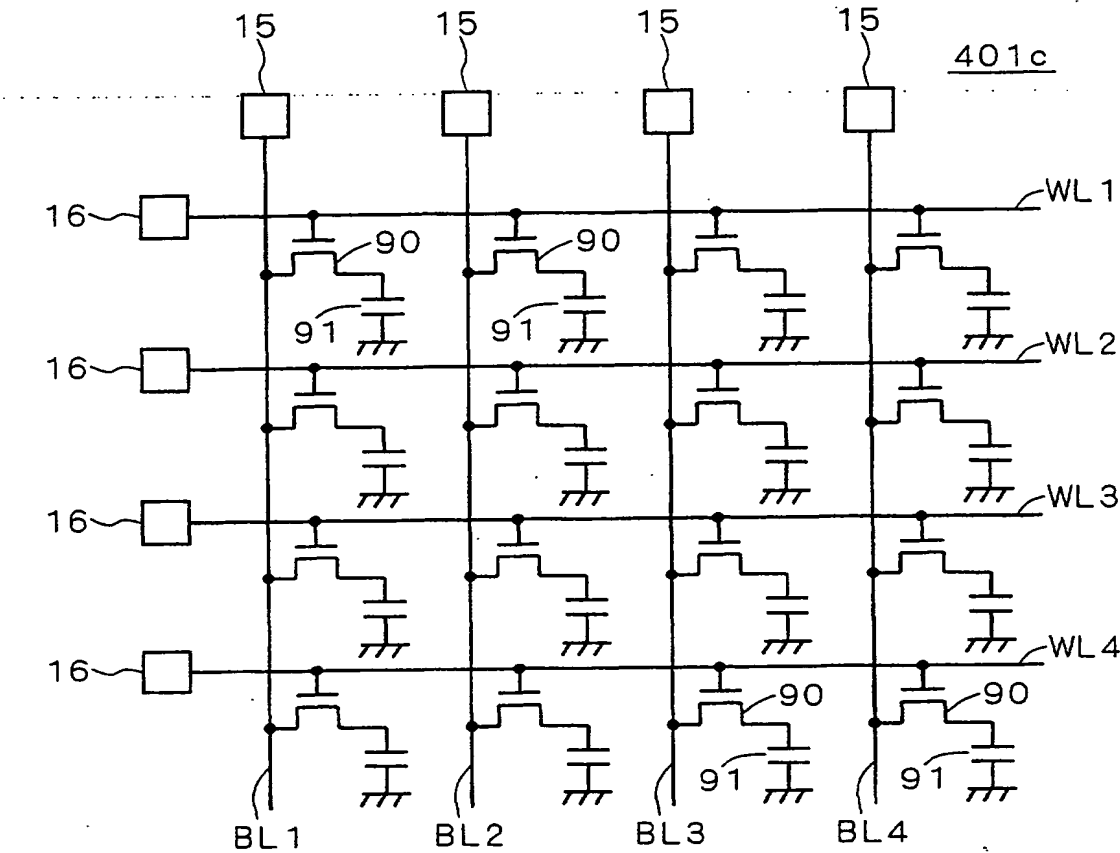


FIG. 63

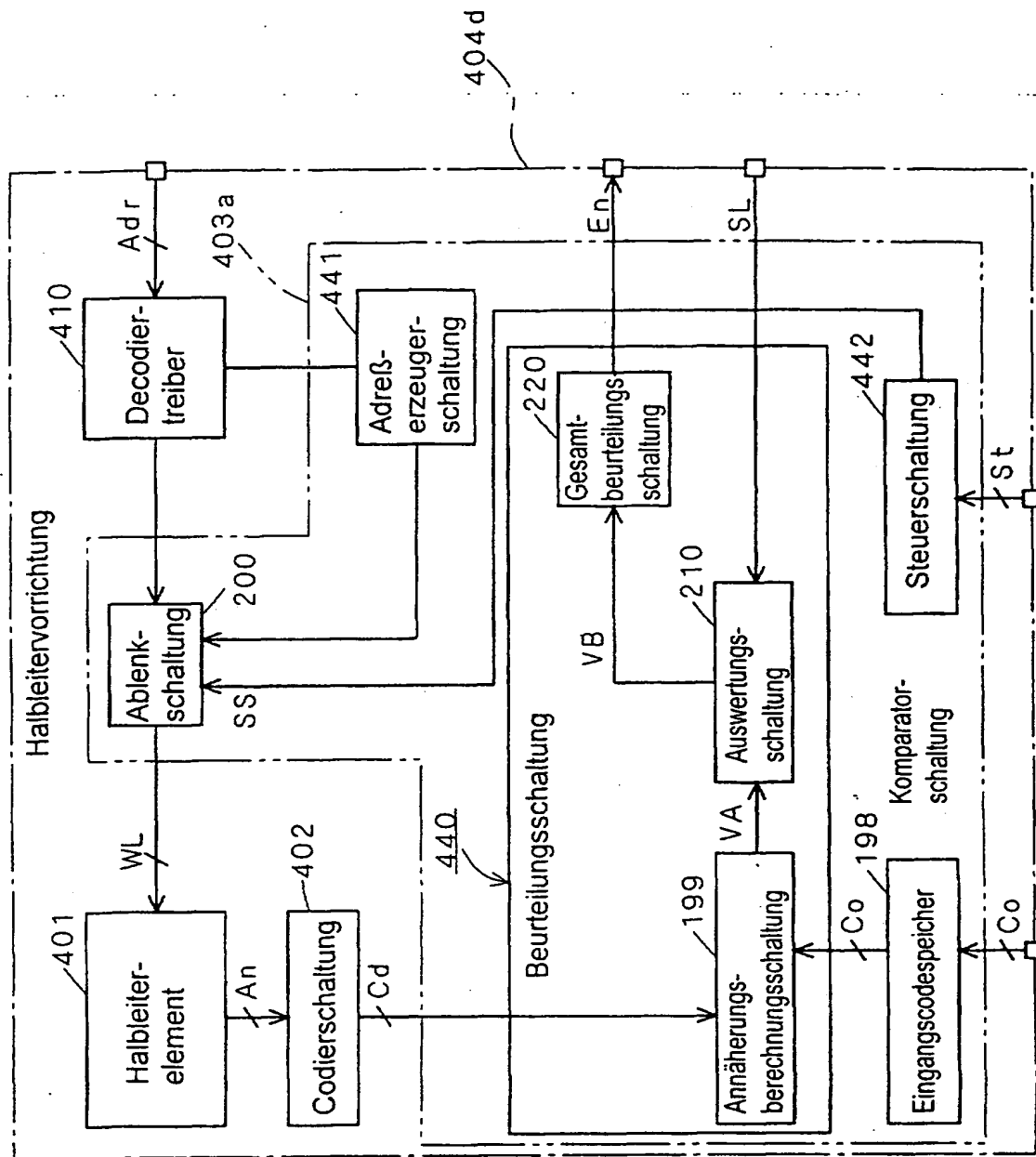


FIG. 64

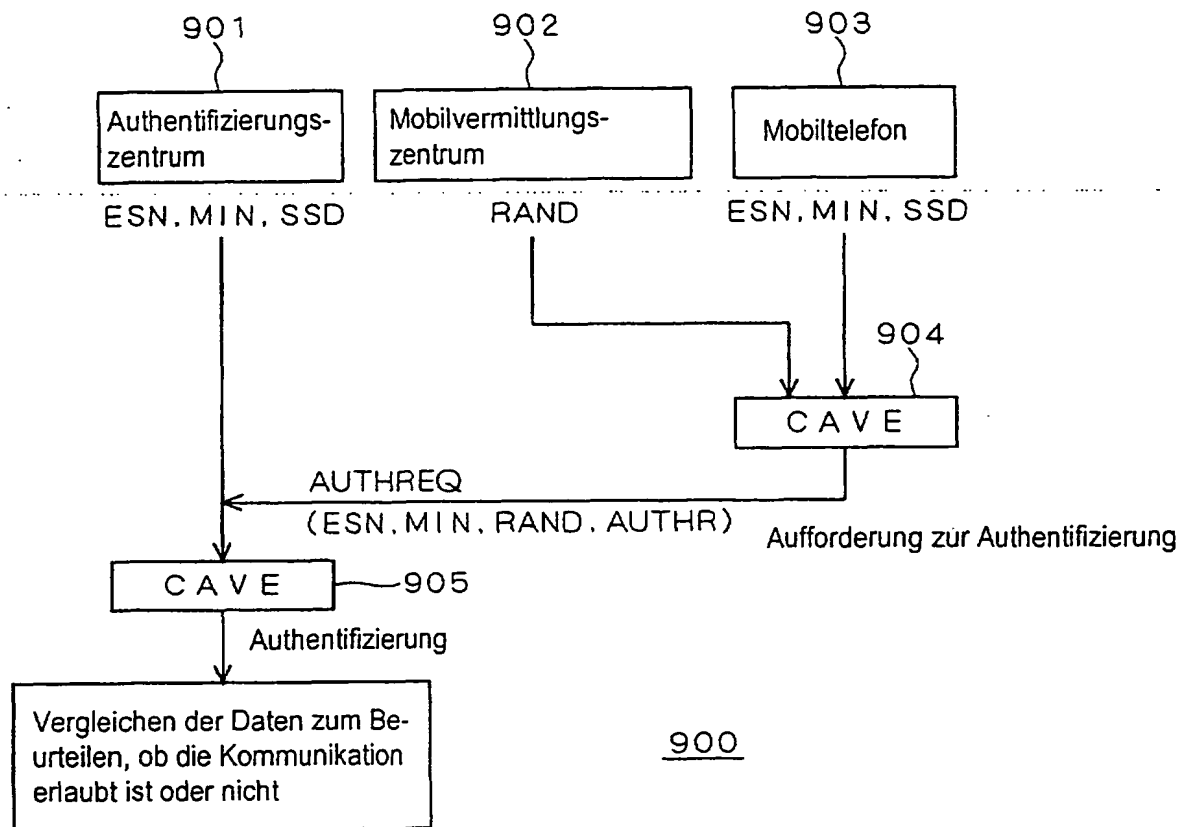


FIG. 65

